JPCERT CC®

2023年度
産業制御システムを対象としたSIRT（制御系SIRT）の実態に関する調査_アンケート回答結果

一般社団法人JPCERTコーディネーションセンター

アンケート実施概要（対象、期間、方式、大項目レベルの主な設問）

- 制御系SIRTの構築状況、体制や機能、活動内容等についての現状や課題を把握するために、一般製造業者を対象として以下に示すアンケート調査を実施した。

調査対象	一般製造業（石油、化学、鉄鋼・製紙、電機・精密、医薬、食品、自動車、機械等）
有効回答数	発出：4,861件 回答：　185件 集計：　185件
調査項目数	105項目
調査項目	1. 基本情報 2. 制御システムの保有状況 3. 「制御システムインシデント」に備えた体制作りの取組状況 4. 実際の制御システムインシデントへの対応状況
調査手法	アンケート調査
調査期間	2023年12月18日～2024年1月26日

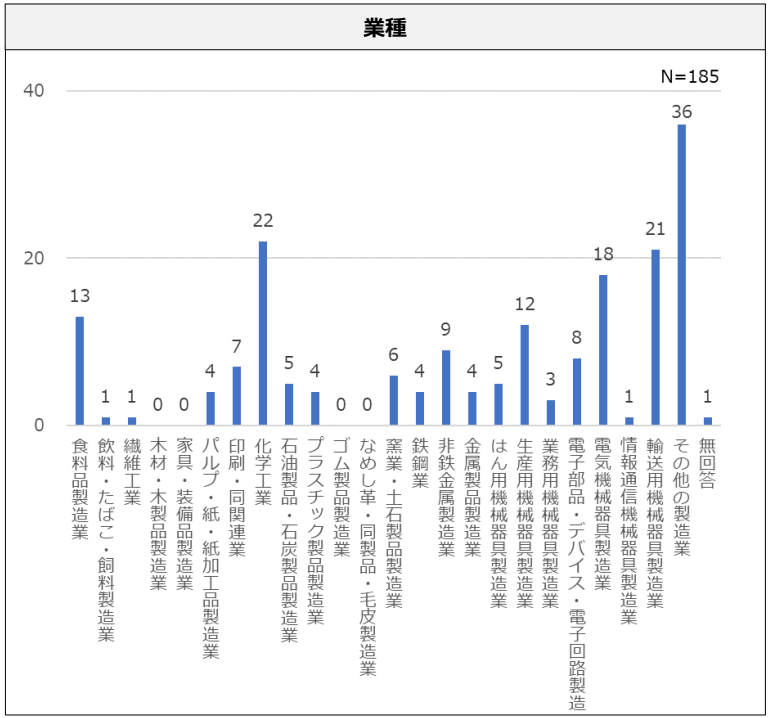
アンケート設問の概要

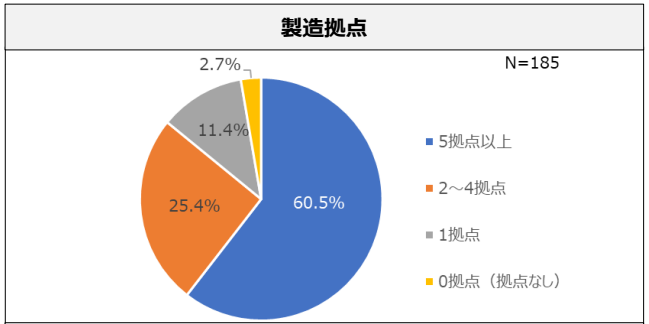
カテゴリー	設問	設問の目的
基本情報	1-1 回答者情報（企業名、回答者所属、連絡先）	アンケート回答者の連絡先把握
	2-1 企業情報（企業概要、企業諸元）	アンケート回答者の属性把握
製造システムの保有状況	3-1 FA製造システムの保有状況	アンケート対象者の選別（FAシステム保有者）
	3-2 PA製造システムの保有状況	アンケート対象者の選別（PAシステム保有者）
	3-3 その他製造システムの保有状況	アンケート対象者の選別（その他システム所有者）
「制御システムインシデント」に備えた体制作りの取組状況	4-1 制御システムインシデントを対象とした取組体制やルール	インシデント発生時の社内の対応ルール・組織・体制の実態把握
	4-2 制御システムインシデント対応体制の取組の対象システム	対応体制が対象とするシステムそのもの及びシステムの重要度の把握
	4-3 制御システムインシデント対応体制の取組内容	平時における制御システムインシデント発生時の取り組み検討、整備具合の把握
	4-4 制御システムインシデントへの取組理由や現状評価、将来像など	制御システムインシデントに対する対策のきっかけ、今後の課題の把握
実際の制御システムインシデントへの対応状況	5-1 制御システムインシデントの発生状況	具体的な被害発生状況の把握
	5-2 制御システムインシデントの被害内容	具体的な被害内容の把握
	5-3 制御システムインシデントの発見経緯と対応内容	具体的な被害発生経緯及び被害対応の把握
	5-4 制御システムインシデントへの対処内容	インシデントの収拾対処の把握
	5-5 制御システムインシデントに対する追加のセキュリティ対策やその評価	被害対応の評価の把握

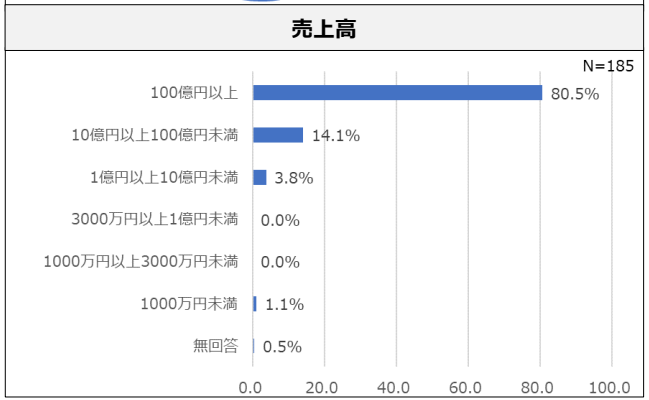
設問番号：1-1、2-1

回答者の属性情報（業種、製造拠点数、売上高）

質問	貴社の業種、製造拠点の有無や数、売上高をお答えください。
回答形態	単一回答
自由記述欄	なし



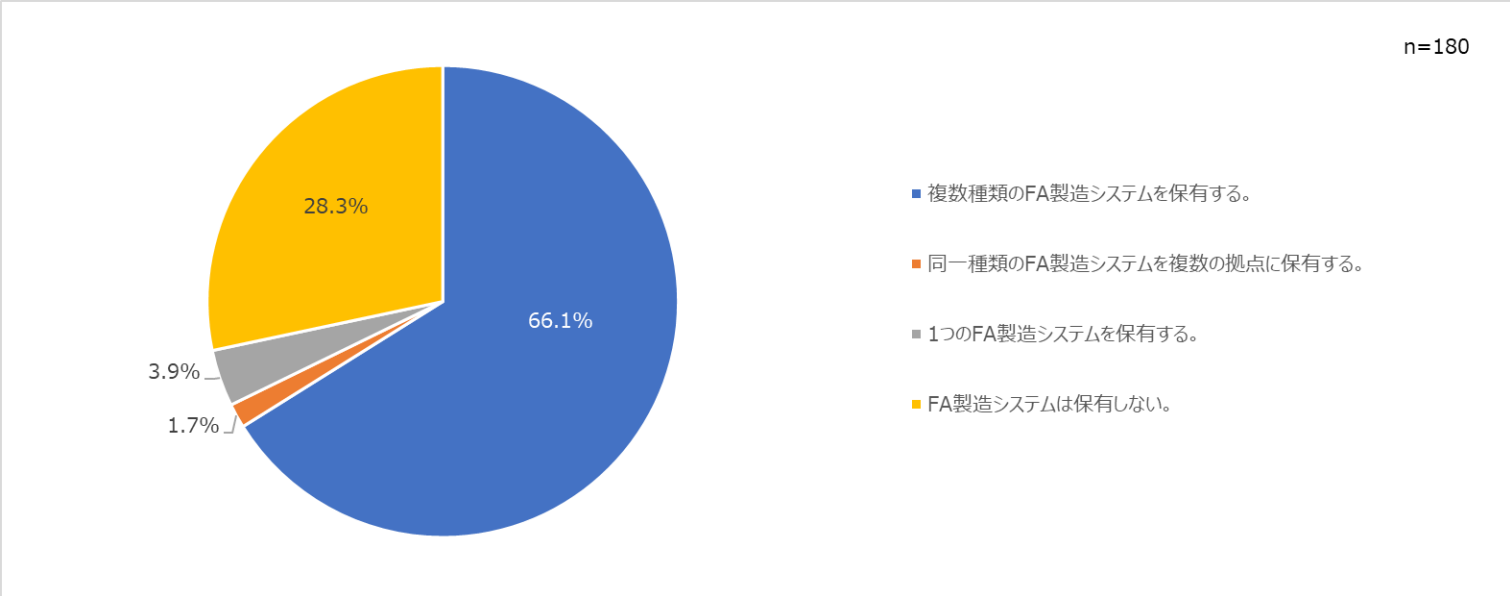




設問番号：3-1-1

回答者のFA製造システムの保有状況

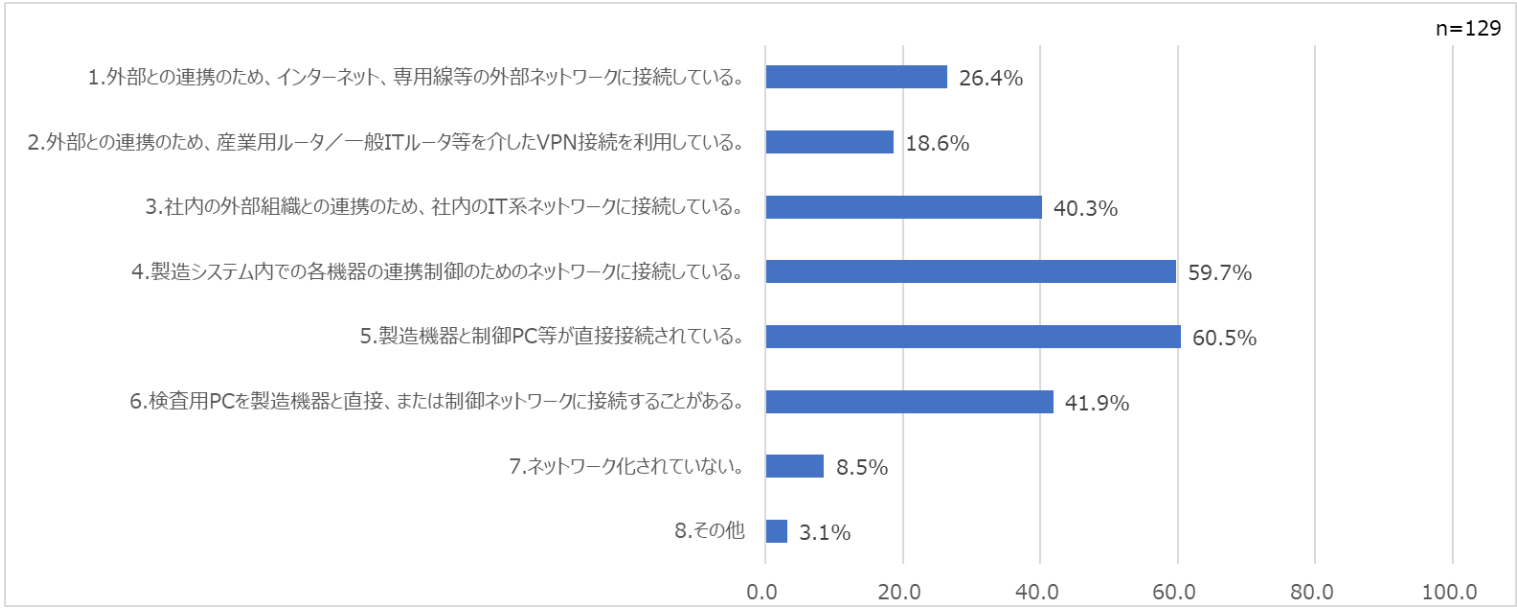
質問	貴社の製造拠点におけるFA製造システム（製造工程を持つライン）の保有状況をお知らせください。
回答形態	単一回答
自由記述欄	なし



設問番号：3-1-2

FA製造システムのネットワーク化状況（1/2）

質問	そのFA製造システムのネットワーク化の状況をお答えください。複数のFA製造システムを保有する場合は、そのいずれかで該当するものがあれば、それをお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：3-1-2

FA製造システムのネットワーク化状況（2/2）

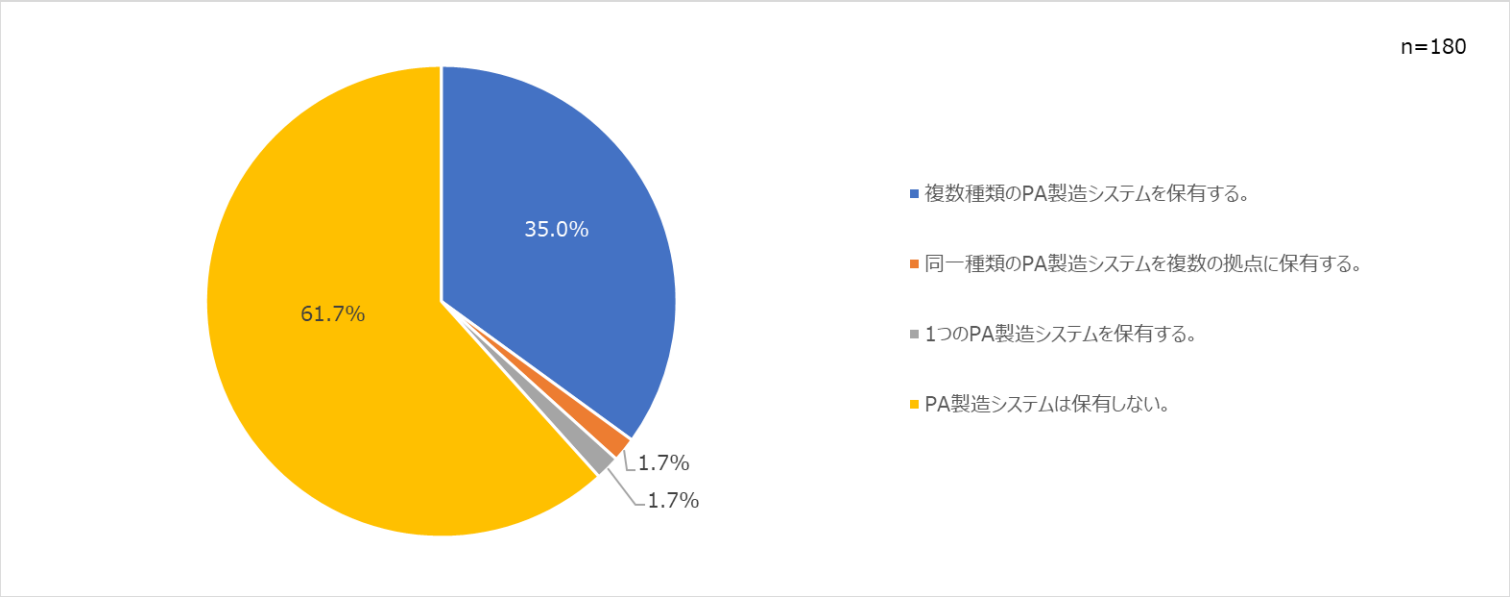
選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 1～7のいずれのケースも存在する。多くは3～5であるが、6、7もある。 1、2については少ないが、一部利用している箇所はある。 • 7：単体設備あり。 • 工場及び製造機器によって異なるが、基本的に3まではどの工場でも該当し、一部装置では2が該当、一部工場では1が該当する。 • 工場ネットワークと事務系ネットワークをF/W経由で接続。 • 複数工場があり、それぞれ異なる。1、3、4、5、6、7は工場ごとで存在している。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：3-2-1

回答者のPA製造システムの保有状況

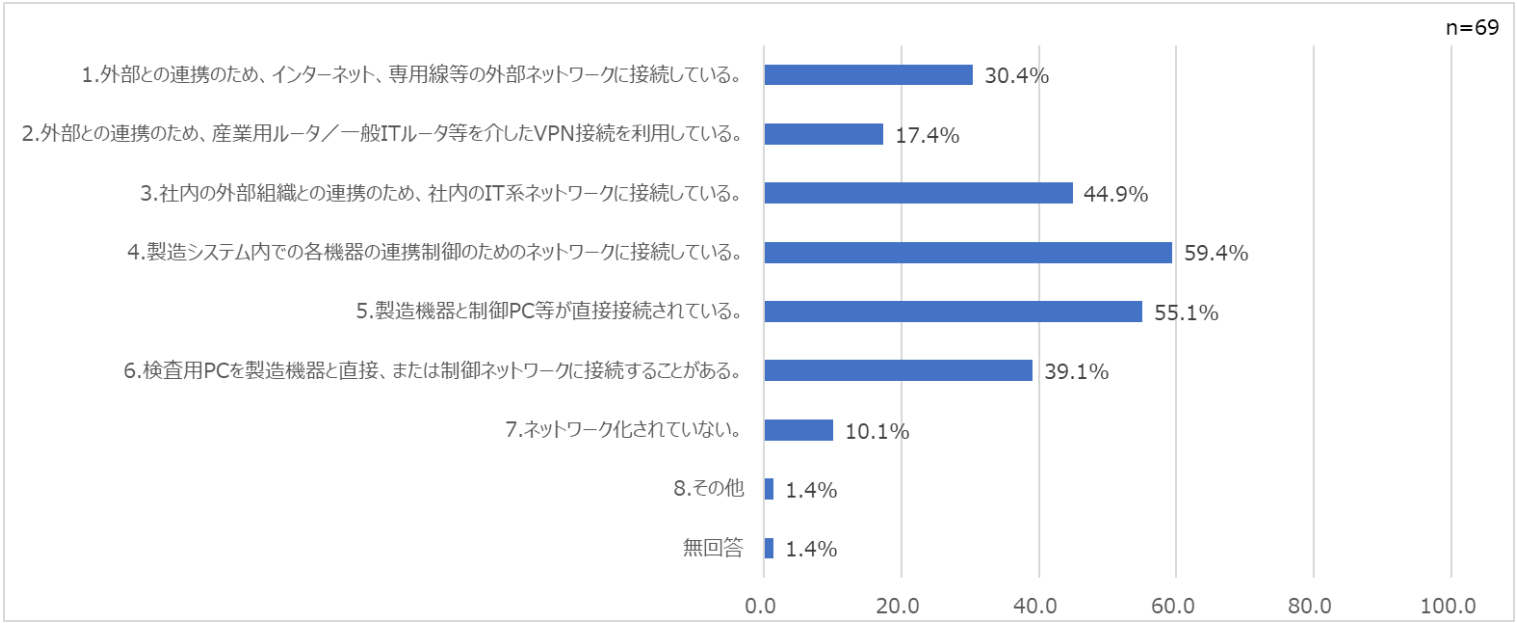
質問	貴社の製造拠点におけるPA製造システム（製造工程を持つライン）の保有状況をお知らせください。
回答形態	単一回答
自由記述欄	なし



設問番号：3-2-2

PA製造システムのネットワーク化状況（1/2）

質問	そのPA製造システムのネットワーク化の状況をお答えください。複数のPA製造システムを保有する場合は、そのいずれかで該当するものがあれば、それをお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：3-2-2

PA製造システムのネットワーク化状況（2/2）

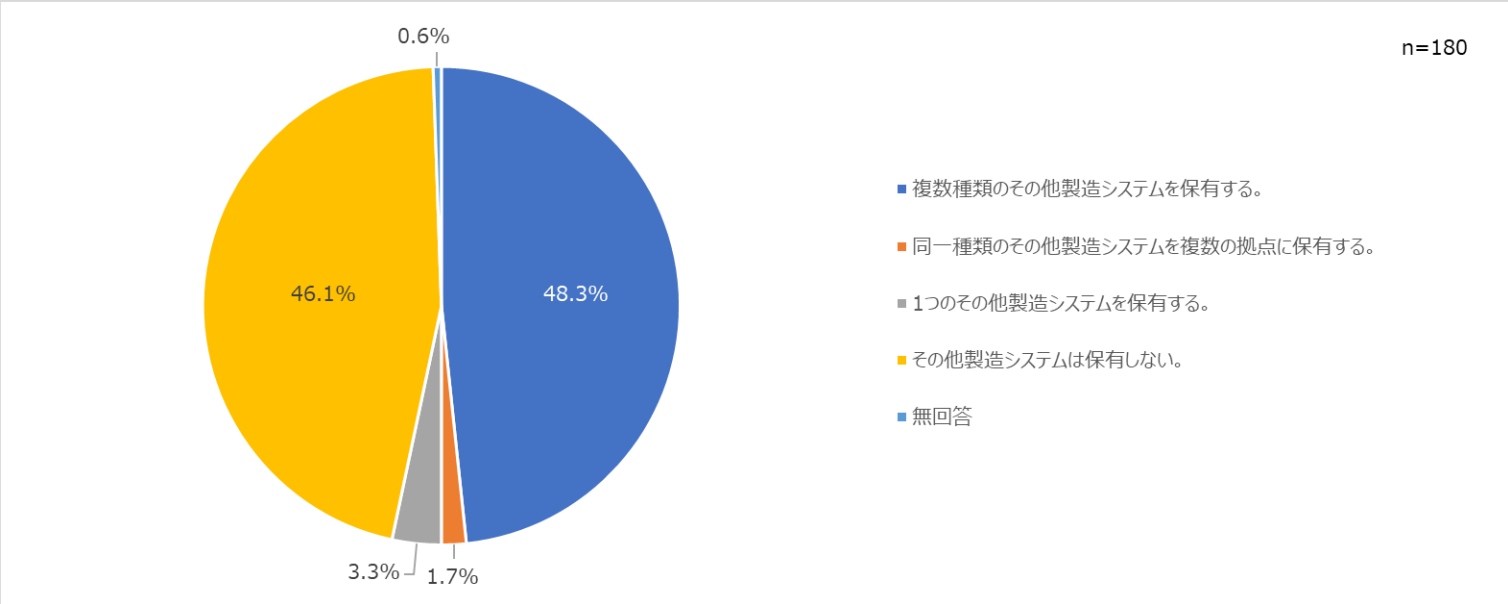
選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 1～7のいずれのケースも存在する。多くは3～5であるが、6、7もある。 1、2については少ないが、一部利用している箇所はある。 • 3：FWを介して接続している。 • 4：塗装工場、鋳鍛工場、樹脂工場を想定 • 7：単体設備あり。 • 工場及び製造機器によって異なるが、基本的に3まではどの工場でも該当し、一部装置では2が該当、一部工場では1が該当する。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：3-3-1

回答者のその他製造システムの保有状況

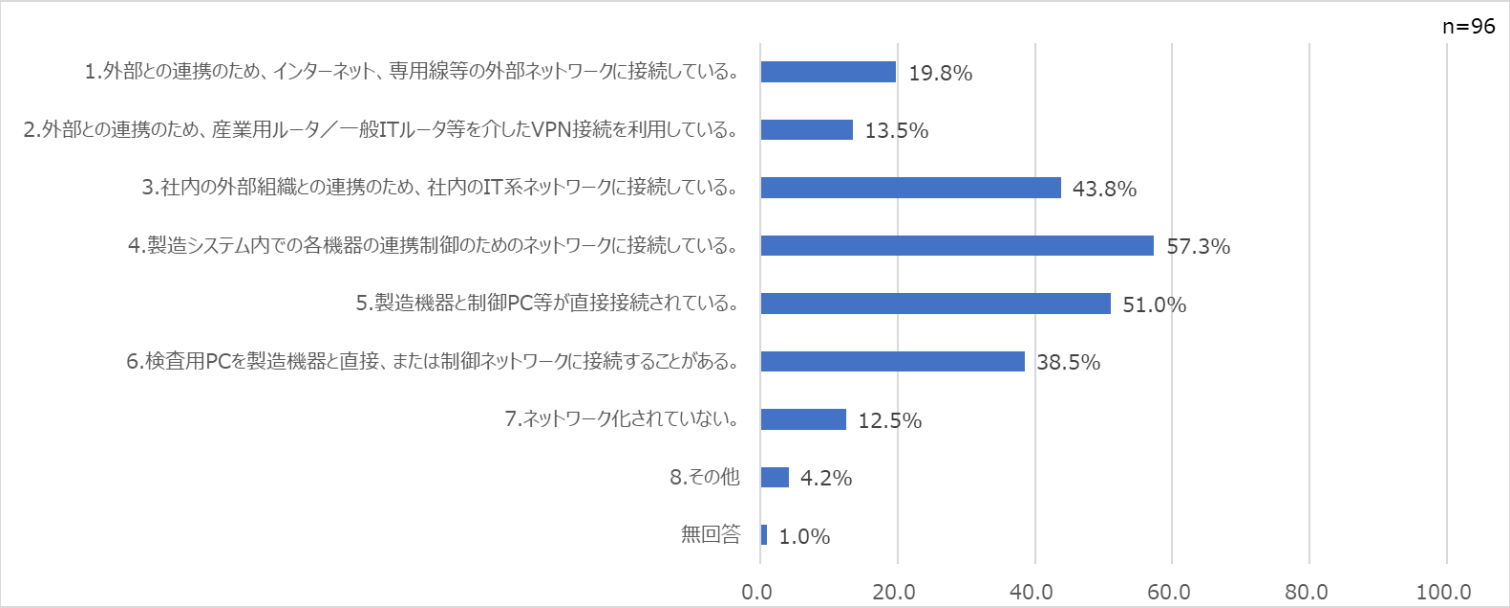
質問	貴社の製造拠点におけるその他製造システム（製造工程を持つライン）の保有状況をお知らせください。
回答形態	単一回答
自由記述欄	なし



設問番号：3-3-2

その他製造システムのネットワーク化状況（1/2）

質問	その他製造システムのネットワーク化の状況をお答えください。複数のその他製造システムを保有する場合は、そのいずれかで該当するものがあれば、それをお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：3-3-2

その他製造システムのネットワーク化状況（2/2）

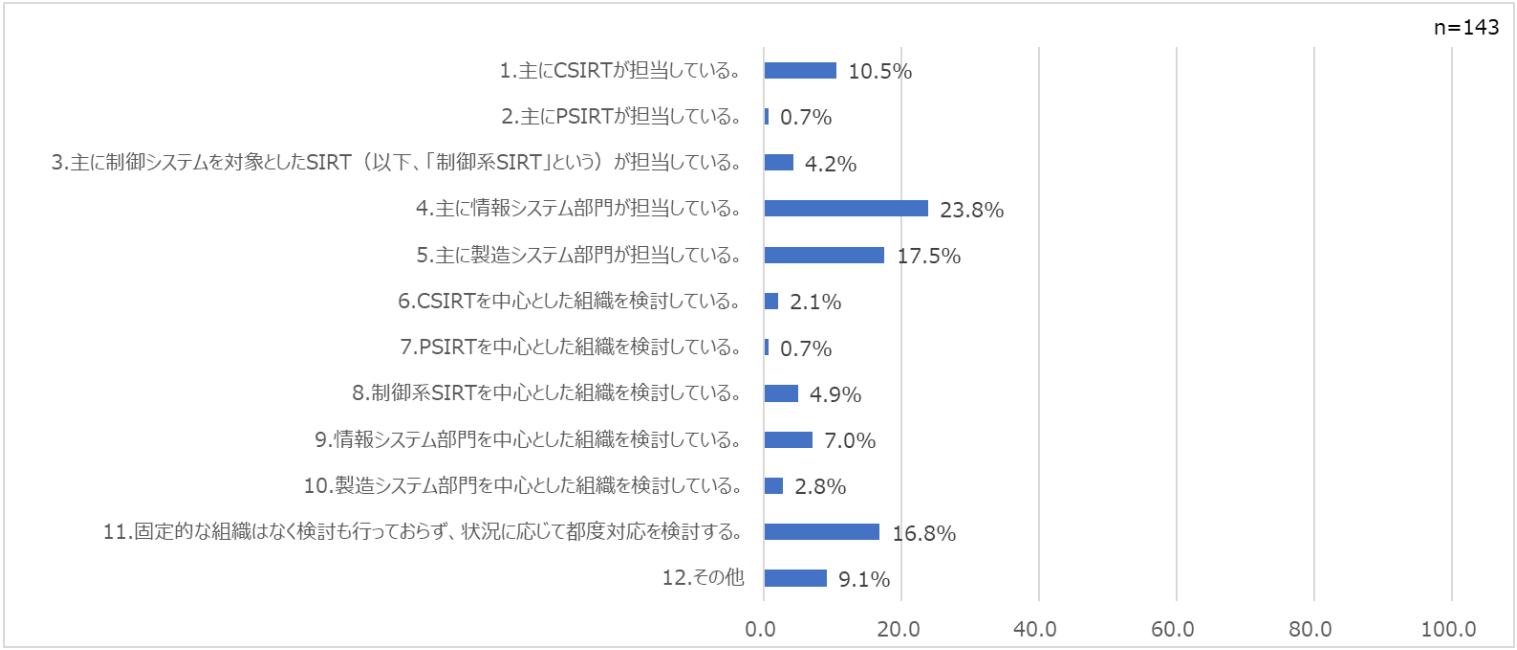
選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• FA、PA、その他の違いが理解できず回答なし（DCS、MES、LIMSはあり）。 • 1～7いずれのケースも存在する。多くは3～5であるが、6、7もある。 1、2については少ないが、一部利用している箇所はある。 • 工場ネットワークと事務系ネットワークをF/W経由で接続。 • 複数工場があり、それぞれ異なる。1、3、4、5、6、7は工場ごとで存在している。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：4-1-1

制御システムインシデント対応体制（1/2）

質問	貴社の制御システムでセキュリティインシデントが起きた場合、主に対応する組織・体制（以下、「制御システムインシデント対応体制」という）は、選択肢の中でどこでしょうか（実体組織以外に仮想的な体制も含みます）。現時点で対応体制はないが、検討中の場合についても、その旨をお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：4-1-1

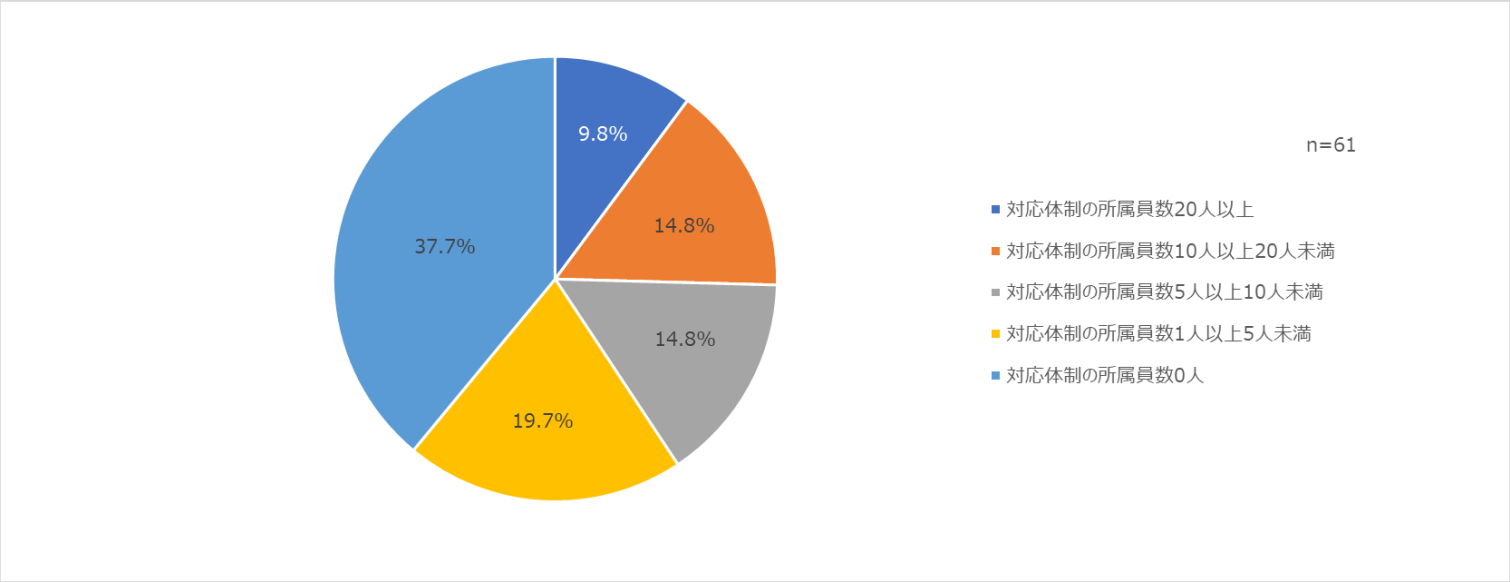
制御システムインシデント対応体制（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• CSIRTおよびPSIRTを一つの部門にしている部門にて対応する。 • CSIRTと工場のシステム部門、エンジニア部門を中心とした組織が担当している。 • 主に製造部が担当している。 • サイバーセキュリティを統括する部門内の制御システムセキュリティ担当が対応している。 SIRT組織ではないが、事実上の制御系SIRTとしての業務を担っており、CSIRTと連携して活動している。 • システム部門の情報・指示に基づき、保守部門が一時対応を行う。二次対応としてシステム部門で対策を検討・実施する。 • 情報システム部門と現場（製造部門）で共同して担当している。 • 製造部門と情報システム部門で連携して対応。 • 製造部門と情報セキュリティ部門が連携。 • 現状は製造システム部門が担当しているが、今後は情報システム部門と製造システム部門で共同した組織を検討している。 • 今後、体制を検討する。 • 主として製造部門が担当するが、CSIRTも入る。 • 情報システム部門がインシデントの内容次第でCSIRTの設置要否を決定し、CSIRTが設置された場合はCSIRTが中心となる。 それ以外では、情報システム部門が中心となり担当する。 • 制御システムとして甚大な被害となりうるケースは無く制御系SIRTは不要と考えている。

設問番号：4-1-2

制御システムインシデント対応体制の組織構成（所属員数）

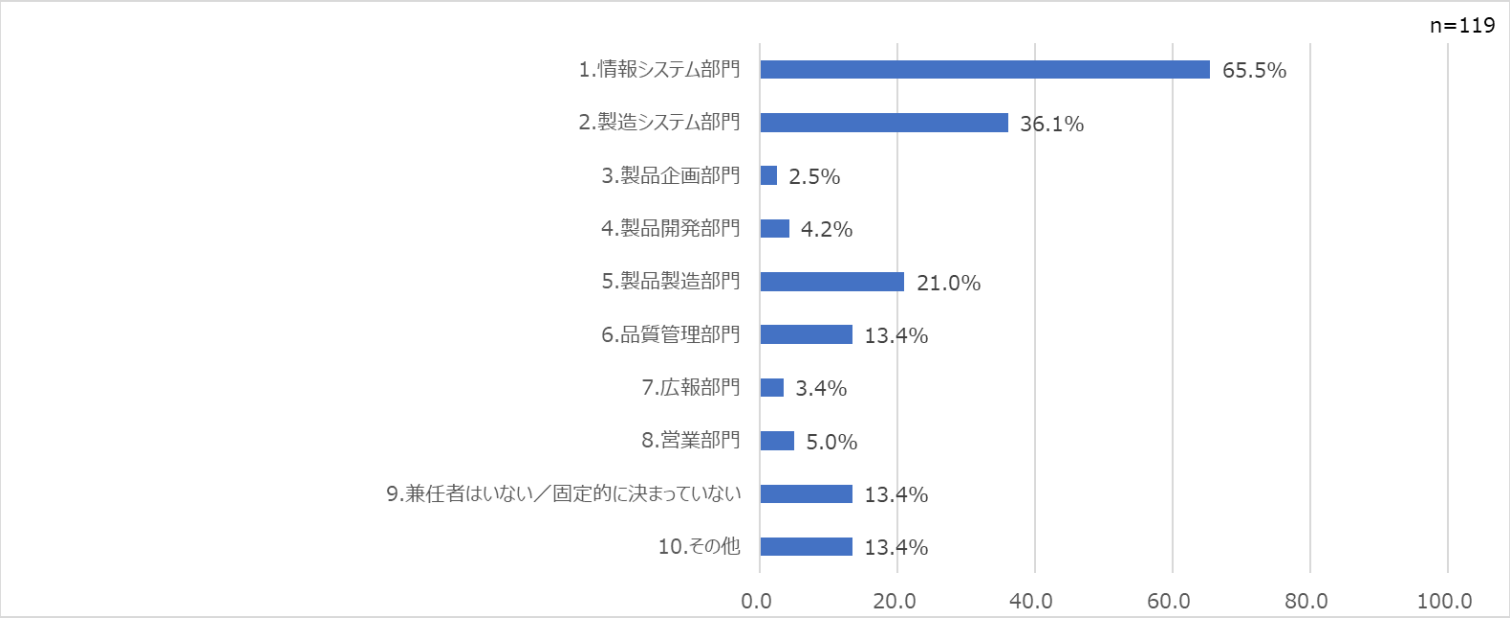
質問	貴社の制御システムインシデント対応体制の所属員数、そのうちの専任者数をお答えください。
回答形態	自由記述
自由記述欄	あり



設問番号：4-1-3

制御システムインシデント対応体制の組織構成（兼任者）（1/2）

質問	貴社の制御システムインシデント対応体制の兼任者の所属部署をお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：4-1-3

制御システムインシデント対応体制の組織構成（兼任者）（2/2）

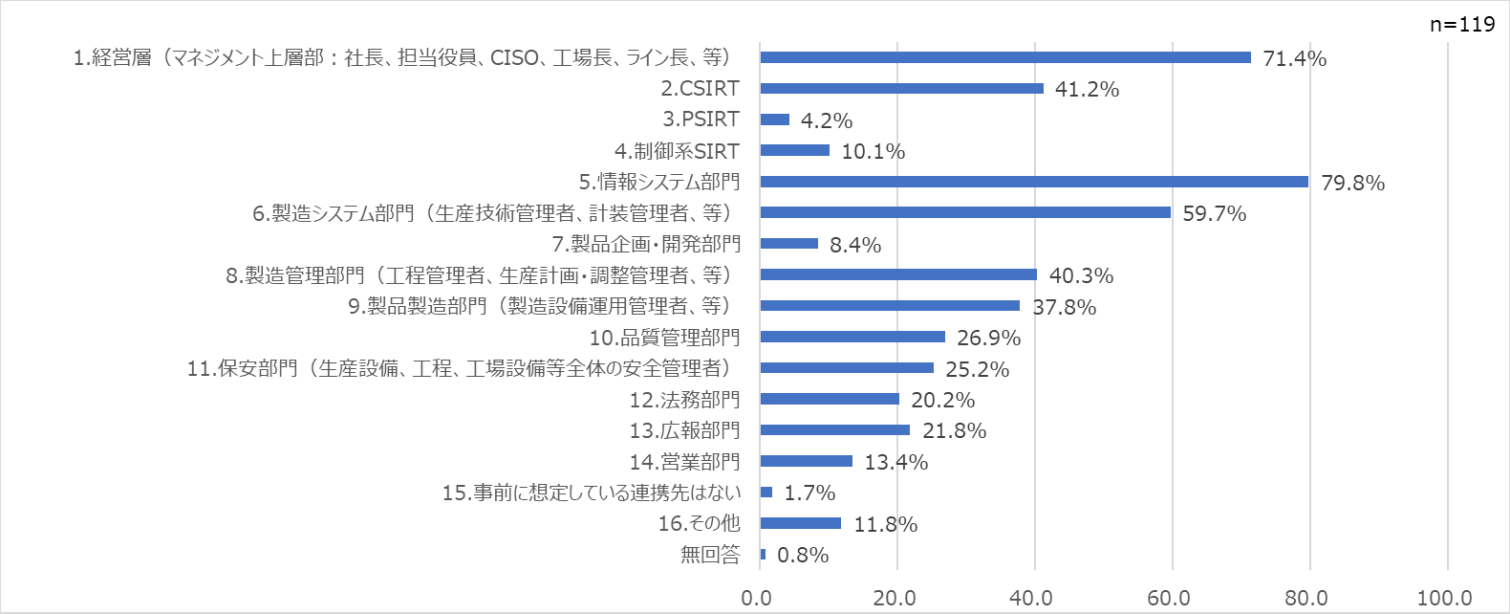
選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• CSIRT • エンジニアリング部門。 • 主に製造部が担当している。 • 固定的に決まっていない。 • 設備管理部門。 • 総務部。 • 技術企画部門。 • 経営企画室。 • 制御系SIRTは存在していない。 • 生産技術部門。 • 製造設備部門。 • 設備部門。 • 1、2：予定。 • 1：検討中。 • 1：システム部門、2：生産技術部、5：保守部門。 • 法務部門。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：4-1-4

制御システムインシデント対応体制の組織構成（連携先）（1/2）

質問	貴社における「制御システムインシデント」への対応準備に当たって、制御システムインシデント対応体制が連携する（連携する可能性のある）部署はどこですか（例えば、連携先としてルール等で定められている部署はどこですか）。
回答形態	複数回答
自由記述欄	あり



設問番号：4-1-4

制御システムインシデント対応体制の組織構成（連携先）（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• サイバーセキュリティ部門。 • 設計部門。 • 設備維持管理部門。 • 1、5、6：予定。 • 1：検討中。 • リスク管理部門。 • リスクマネジメント部。 • 監査部門。 • 危機管理部門。 • 情報セキュリティ委員会。 • 親会社情報システム部門。 • 制御系SIRTは不要と考えている。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：4-1-5

体制やルール、技術上の工夫点や留意点等（1/2）

質問	貴社では制御系SIRT以外が制御システムインシデントを取扱うにあたって、体制やルール、技術上の工夫点や留意点等がありましたらお答えください。
回答形態	自由記述
回答数	32
個社回答	• CSIRTが中心になって対応している。 • CSIRTでサポート。 • 意識統一含め、まだ体制が十分ではない。 • 主に社内インフラを扱う情報システム部門が中心になって対応を進める。 • 外部委託業者と連動し監視、対応、エスカレーションを実施している。 • 各工場で情報システム・セキュリティに関する管理者と担当者（情報系、制御系それぞれに対して）を任命しており、インシデントが発生した際にはこれらのメンバーが本社の情報システム部門と連携をすることで対応としている。 • 各工場の製造設備の電気系担当者を体制に組み込んでいる。 • グループ全社で体制とルールを標準化し、順次、展開中、弊社は順番待ち。 • 現状具体的な体制はなく、今後検討が必要と考えている。 • 現状未定。 • 現場と情報システム部門の円滑な連携体制がとれるように制御系セキュリティに関する社内協議会で各種幹部の情報管理責任者を決めている。また、その中でインシデント対応訓練や監査を実施している。 • 経産省「サイバー・フィジカル・セキュリティ対策ガイドライン」を元に制御システムセキュリティ規準を作成し、体制とルールの確立と浸透を図っている。 • 現時点では取り組み中で、ルールと体制は明確になっていない。現状、生産技術部門、情シス部門、品質管理部門、生産製品の開発部門、PSIRTで対応することになる。 • サイバーセキュリティに関連する部署を中心に各部門と連携する体制としている。 • サイバーセキュリティ規程によりインシデントランク分けを行い、インシデント報告先やタイミングを決めている。 • 社内の情報資産であるため、基本的にはCSIRTの管轄で、実働は製造部門が行う。 • 情報セキュリティに関するインシデントは全て情報セキュリティ運用組織（会社全体の組織）で取り扱う。 • 制御系SIRTではないが、制御システムのサイバーセキュリティを管理する部門を本社に設けて、有事の際には支援する体制をとっている。 • 製品製造部門が対応にあたり、情報システム部門は必要に応じて技術支援を行う。 • セキュリティガイドライン、情報セキュリティ委員会。 • 全社組織として情報セキュリティ委員会を設置し、事務局(情報システム部)と各部門が連携を取るよう体制を整備している。 • 組織上は制御系SIRTが存在するが、リソース的・技術的に具体的なインシデント対応ができていない（情シス部門対応）。全社的にも各部門・拠点的にも拡充を検討する必要がある。 • 体制検討中。 • 体制の整備を企画中。

設問番号：4-1-5

体制やルール、技術上の工夫点や留意点等（2/2）

質問	貴社では制御系SIRT以外が制御システムインシデントを取扱うにあたって、体制やルール、技術上の工夫点や留意点等がありましたらお答えください。
回答形態	自由記述
回答数	32
個社回答	• 担当者がインシデント確認後、都度関係者（部門）へ連絡する。 • 内規に準じて実施している。 • ネットワークについては全社共通のネットワークを使用している。セキュリティ対策は本社で管理運用し連携して対応を行っている。 ネットワークではファイアウォール・ウィルス検知サーバ等でウィルス対策をしている。 • 普段からのコミュニケーションを密に取る。 • わかる人といっしょに取り扱う（予定）。 • 無線機器は使用しない。社外のシステムには繋がない。社内の一般のシステムには繋がない。 • 連絡網の整備（情報システム部門への連絡）。

設問番号：4-1-6

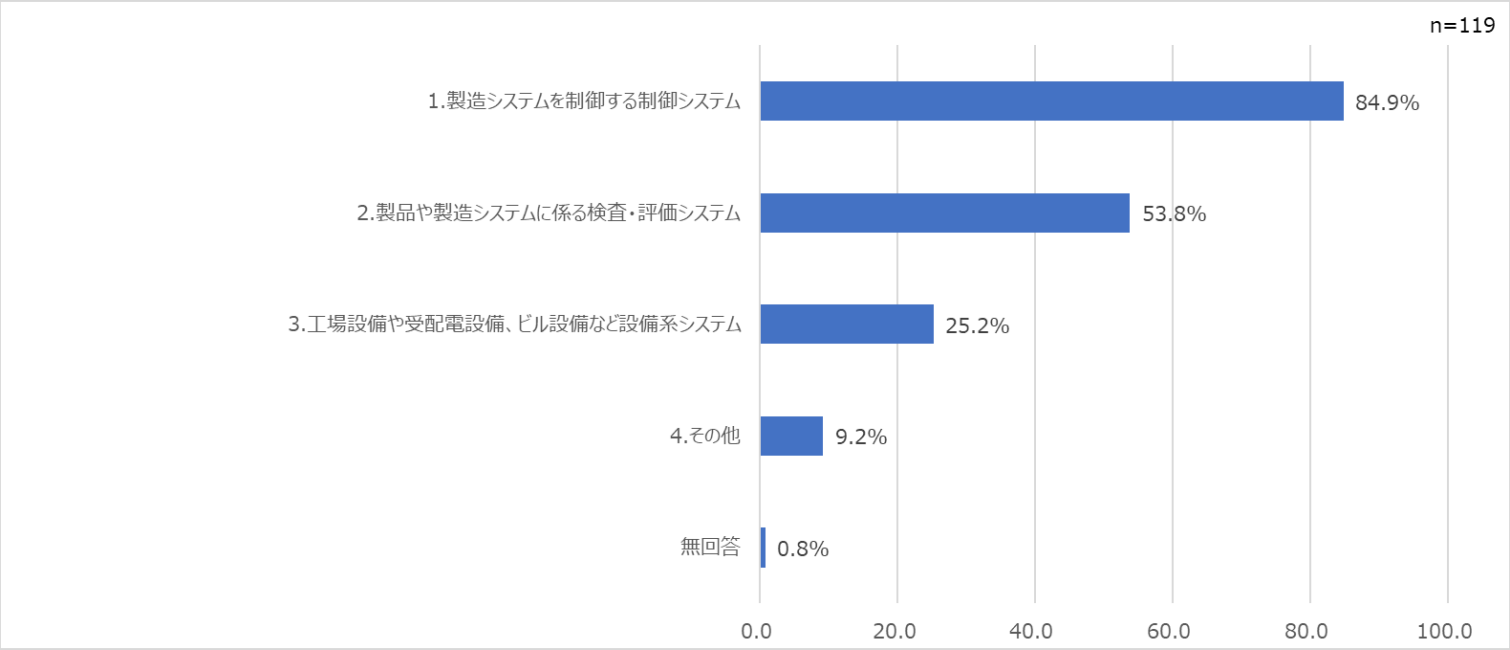
制御システムインシデントを専門に取り扱う部署を組織（検討中を含む）した最大の理由

質問	貴社で制御システムインシデントを専門に取り扱う部署を組織（検討中を含む）した最大の理由についてお答えください。
回答形態	自由記述
回答数	14
個社回答	• 部署は組織していない。制御系（＝工場系）のSIRTを組織した理由としては、工場については、ITとは異なり安易に止めづらい、止めるとしても多方に調整など発生するため、 CSIRTとは独立させる必要があると考えた。 • インシデントを機に、制御系システムを含めた全体のセキュリティ強化を進めている。 • OTが従来のIT管轄部署の所管外であるため。 • インシデント発生時に生産に影響が出るリスクが高くなってきているため。 • インシデント発生時の対応を速やかにおこなえるよう事前の備えとして。 • 親会社からの指示に基づく。 • 海外での制御系インシデントの多発。 • 過去に海外グループ会社の工場で侵害が発生、複数社へ拡散してしまった為、強化を実施。 • 工場内にはITセキュリティの観点や施策がそのまま通用しないため。 • 昨今のサイバー攻撃へ備えるための体制づくりが必須と考えたため。 • 制御系SIRTだけではマンパワーが不足。インシデント対応時は、実際に制御設備を運用管理している計装部門の協力が必要なため。 • 制御系のネットワークの運用や末端部分についてはどうしてもCSIRTの管理が行き届かない規模であるため。 • 製造管理部門独自のシステムが存在し、情報システム部門だけでは調査・復旧が困難であるため。 • 生産設備をよく知っている。

設問番号：4-2-1

制御システムインシデント対応体制が対象としている制御システム（1/2）

質問	貴社の制御システムインシデント対応体制が、その取組の対象としている制御システムはどのようなものでしょうか。
回答形態	複数回答
自由記述欄	あり



設問番号：4-2-1

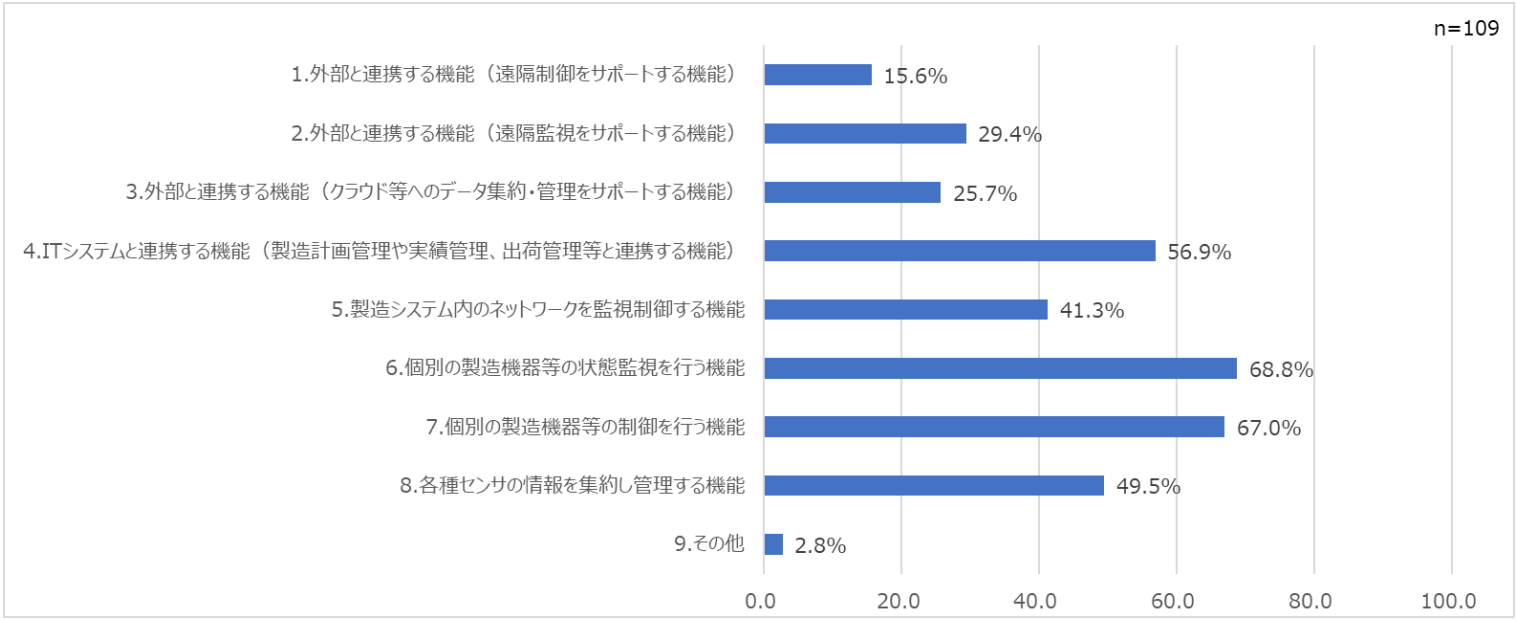
制御システムインシデント対応体制が対象としている制御システム（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 運転データを保存するシステム。 • 研究・開発用の設備・システム。 • 現在、調査中。 • 顧客からの受注部品の小部品展開及び、社内取引先への発注システム。社員給料支払い他。 • 制御系SIRTはない。 • 生産工程・在庫管理システム。 • 全て。 • 特別体制があるわけではない。 • まだ決まっていない。

設問番号：4-2-2

制御システムを構成する機能（システムが有する機能）

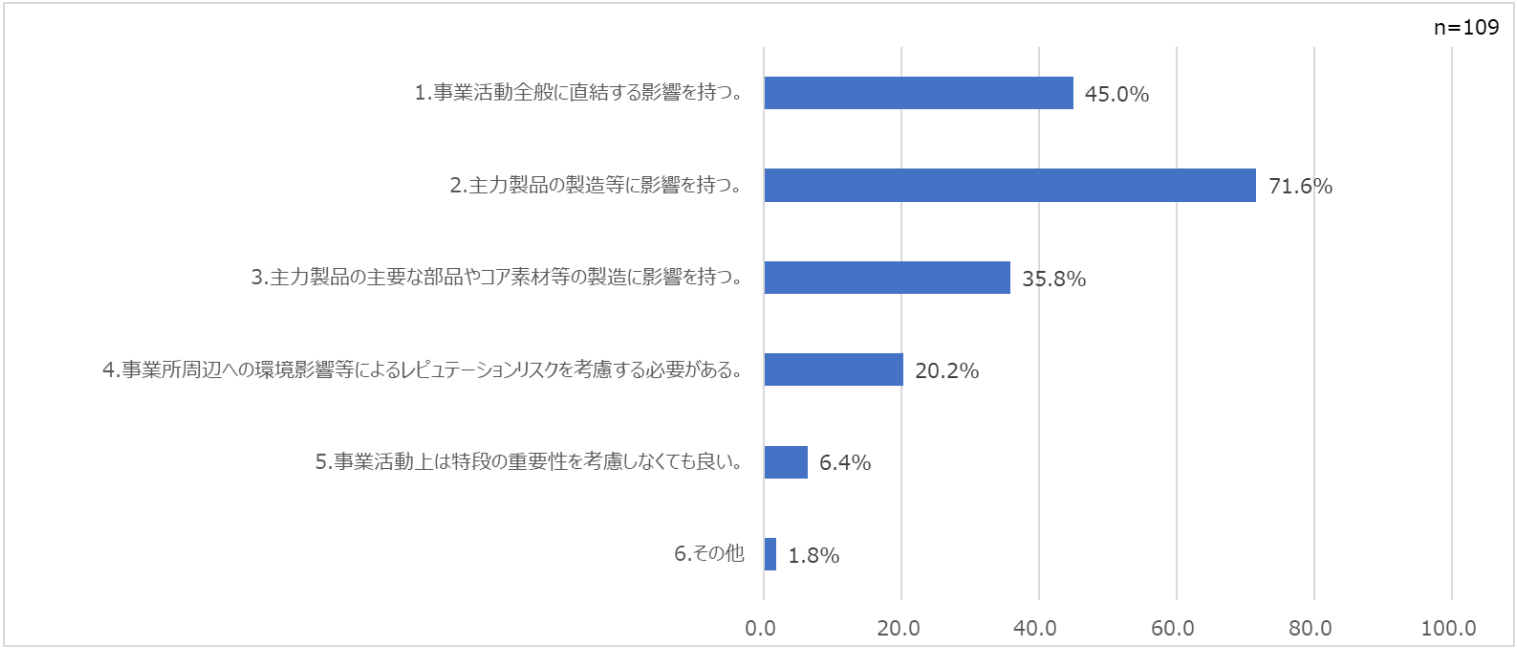
質問	4-2-1にてお答えいただいた制御システムを構成する機能（システムが有する機能）についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：4-2-3

制御システムの事業活動上の重要度

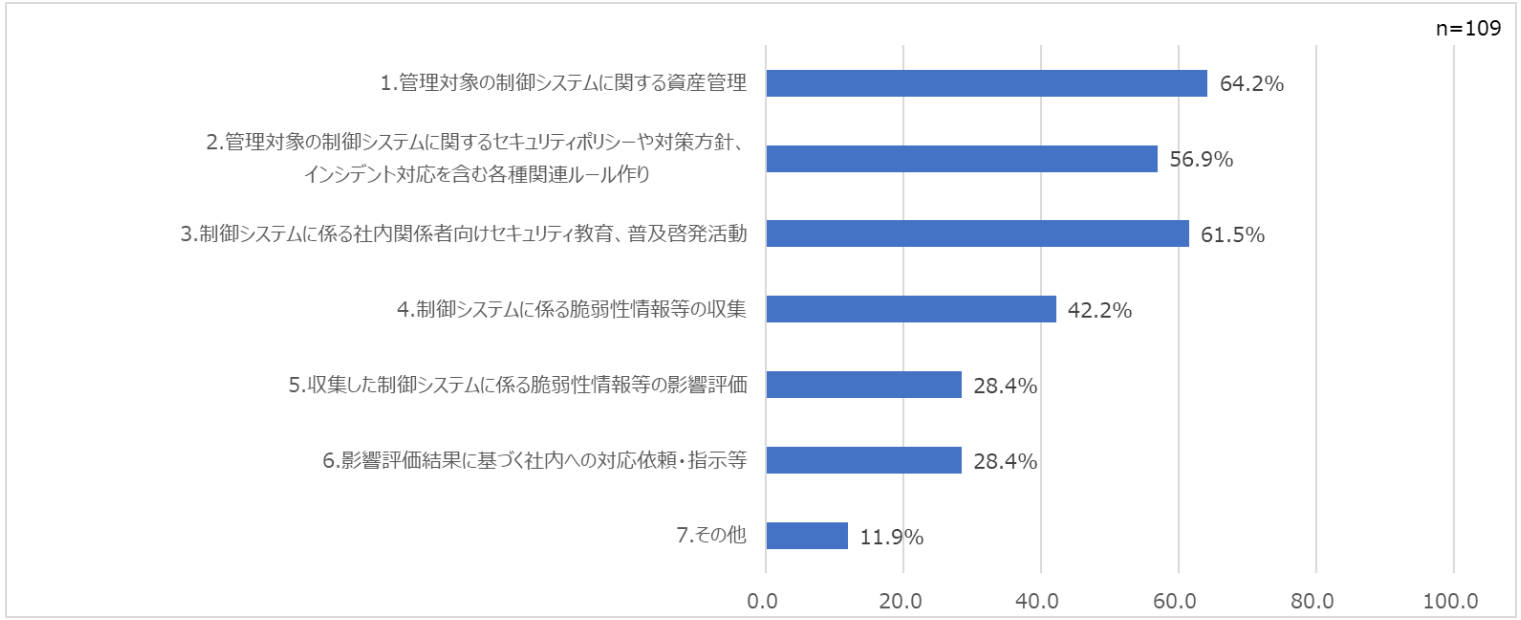
質問	4-2-1にてお答えいただいた制御システムの事業活動上の重要度についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：4-3-1

制御システムインシデント対応体制の日常の取組（1/2）

質問	貴社の制御システムインシデント対応体制が日常的な取組としてどのような活動を実施しているかお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：4-3-1

制御システムインシデント対応体制の日常の取組（2/2）

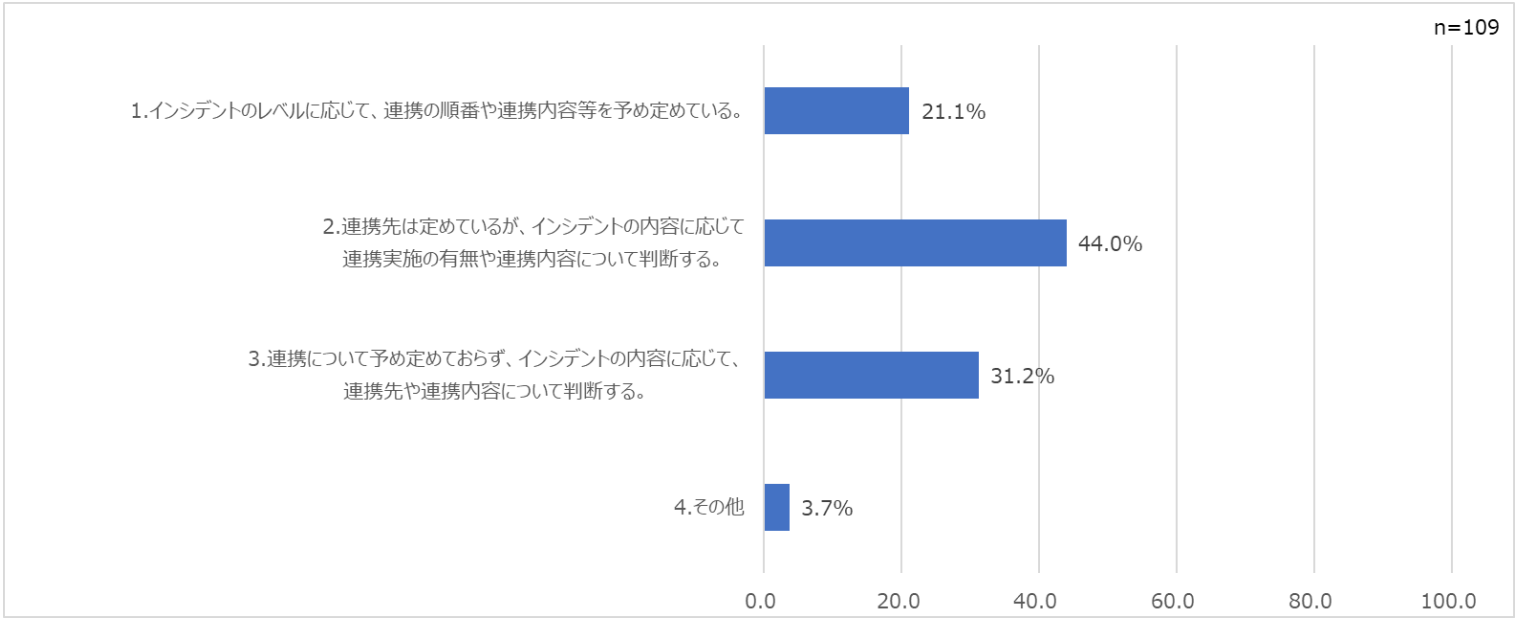
選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• インシデント対応訓練。 • 検討中で日常的な取組は現時点では無い。 • 制御システムインデント対応に関する固定的な組織はない。 • 2：工場設備のシステムに関するセキュリティ要領を策定済み。 • 4・5は全ての制御システムではないが実施しているシステムもある。 • ほとんどできていない。 • 検討中。 • 現在、準備中。 • 現場工場の取り組みは不明。 • 現状は組織形成中。 • 障害対応、維持管理。 • 制御システムのハードニング。 • 制御ネットワークへのセキュリティ製品の導入、運用。 • 体制や役割が決まっていない。 • 特に何もしていない。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：4-3-2

社内外の連携組織との連携ルール（1/2）

質問	貴社の制御システムインシデント対応体制は、制御システムインシデントに備えて、社内外の連携組織との間の連携ルールを定めているかお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：4-3-2

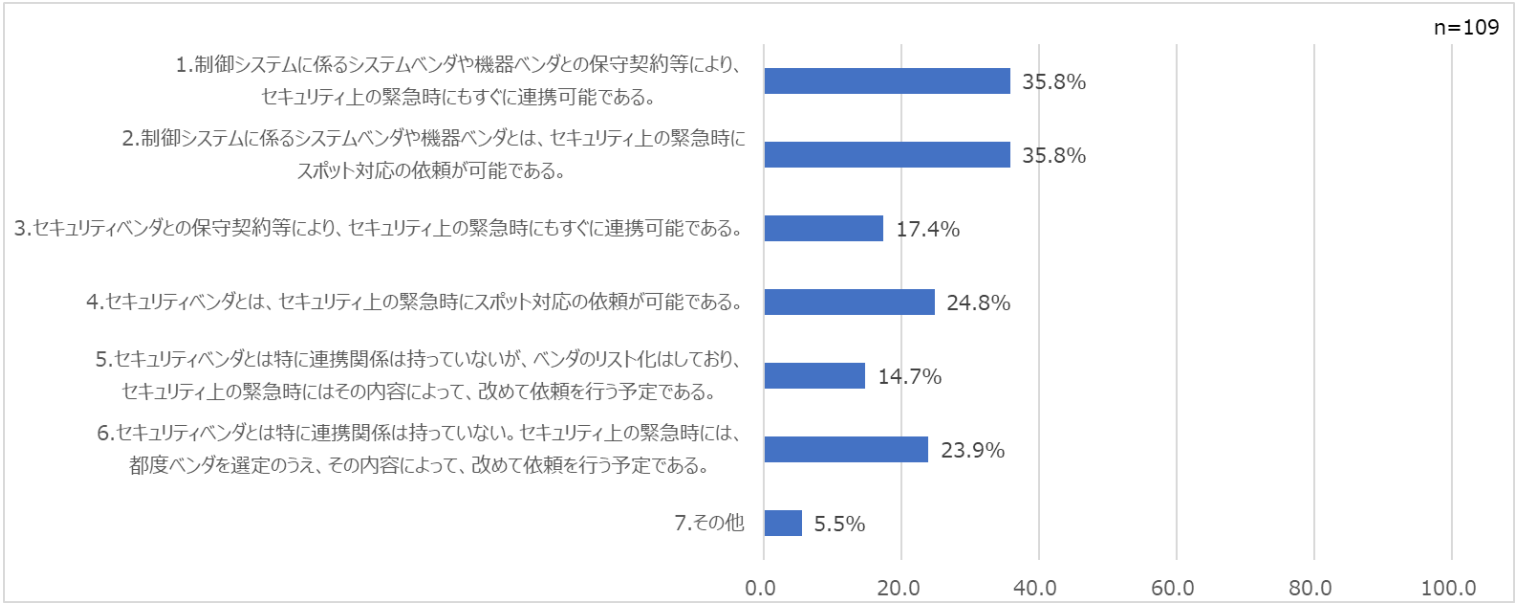
社内外の連携組織との連携ルール（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• CSIRTに準拠。 • 情報セキュリティのエスカレーションルールに準じている。制御系SIRT用はこれから整備予定。 • 制御システムセキュリティ規準ではルールを定めるように記載している。 • ルール・体制を検討中。

設問番号：4-3-3

制御システムインシデントに向けたベンダ等との連携体制（1/2）

質問	貴社の制御システムインシデント対応体制は、制御システムインシデントに備えてベンダ等とどのような日常の連携体制を構築しているか、その程度と併せてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：4-3-3

制御システムインシデントに向けたベンダ等との連携体制（2/2）

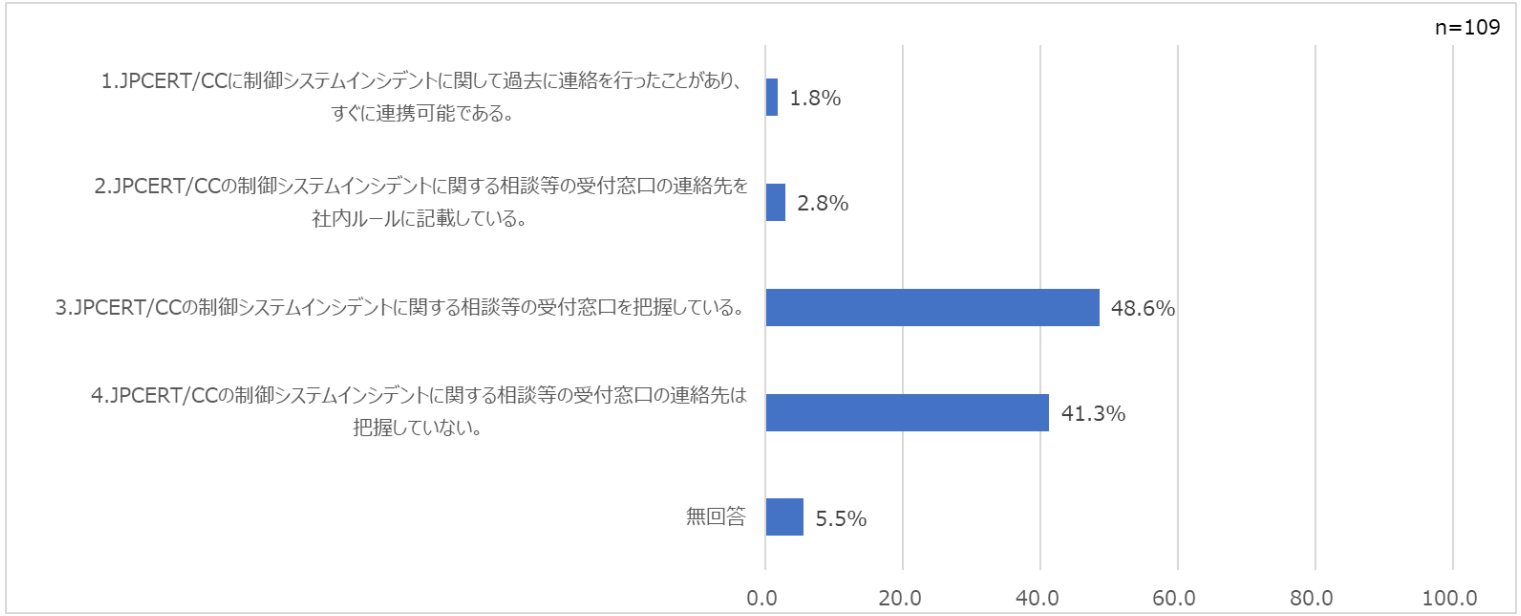
選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 1については一部装置では実施だが全てではない。 • 一部の制御システムでは3まで可能。 • 本社のIT部門が対応する。 • 検討中。 • 自社制御機器を多く使用しているため、自社のPSIRTや製品開発部門との連携は取れている。 • セキュリティベンダとの連携対象はごく一部の制御システムに限る。 • 詳細は不明。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：4-3-4

JPCERT/CCの窓口との連携体制

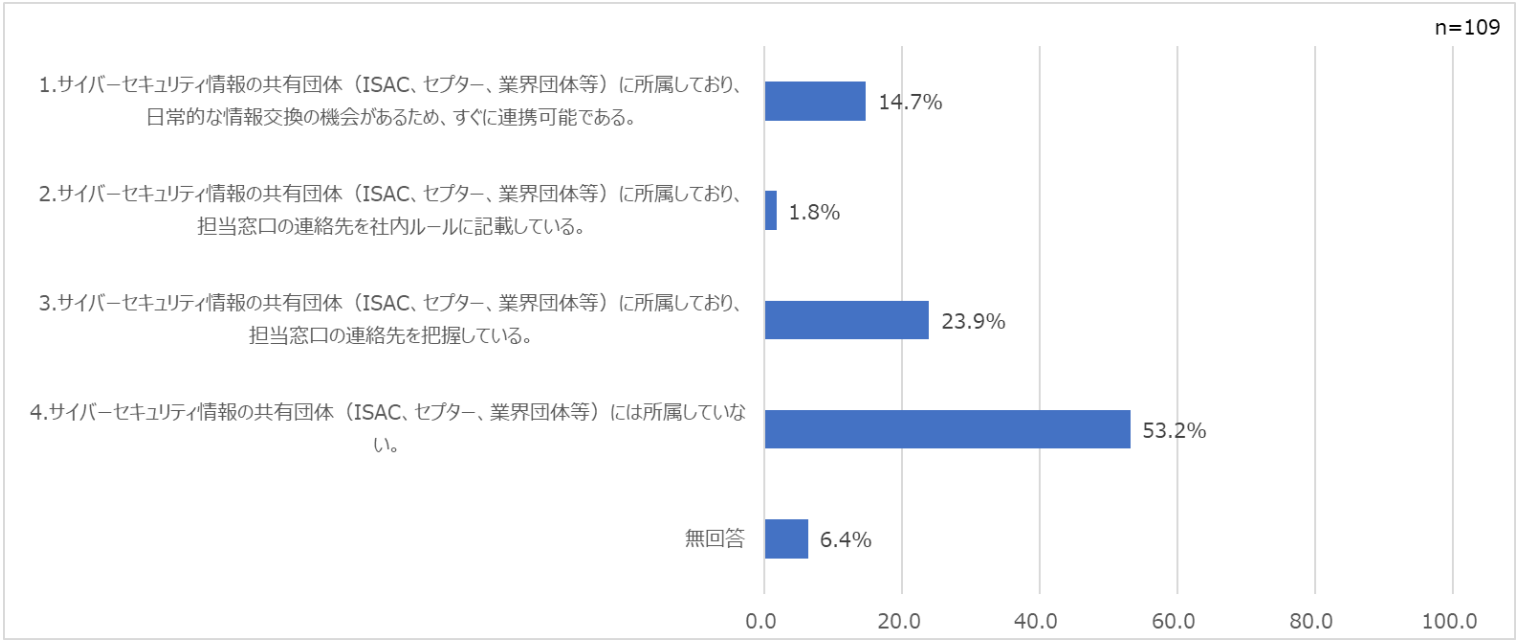
質問	貴社の制御システムインシデント対応体制は、制御システムインシデントに備えて各公的窓口とどのような日常の連携体制を構築しているか、その程度と併せてお答えください。
回答形態	単一回答
自由記述欄	なし



設問番号：4-3-5

サイバーセキュリティ情報の共有団体の窓口との連携体制

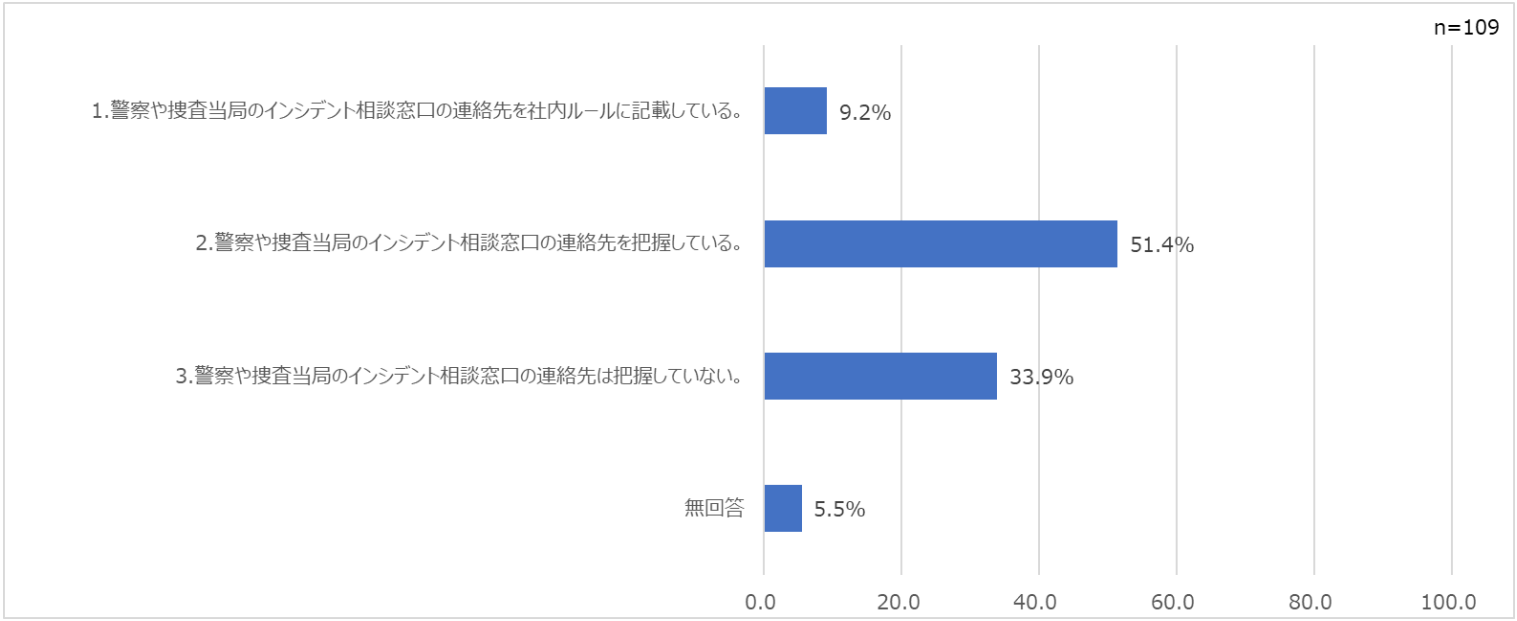
質問	貴社の制御システムインシデント対応体制は、制御システムインシデントに備えて各公的窓口とどのような日常の連携体制を構築しているか、その程度と併せてお答えください。
回答形態	単一回答
自由記述欄	なし



設問番号：4-3-6

警察や捜査当局の窓口との連携体制

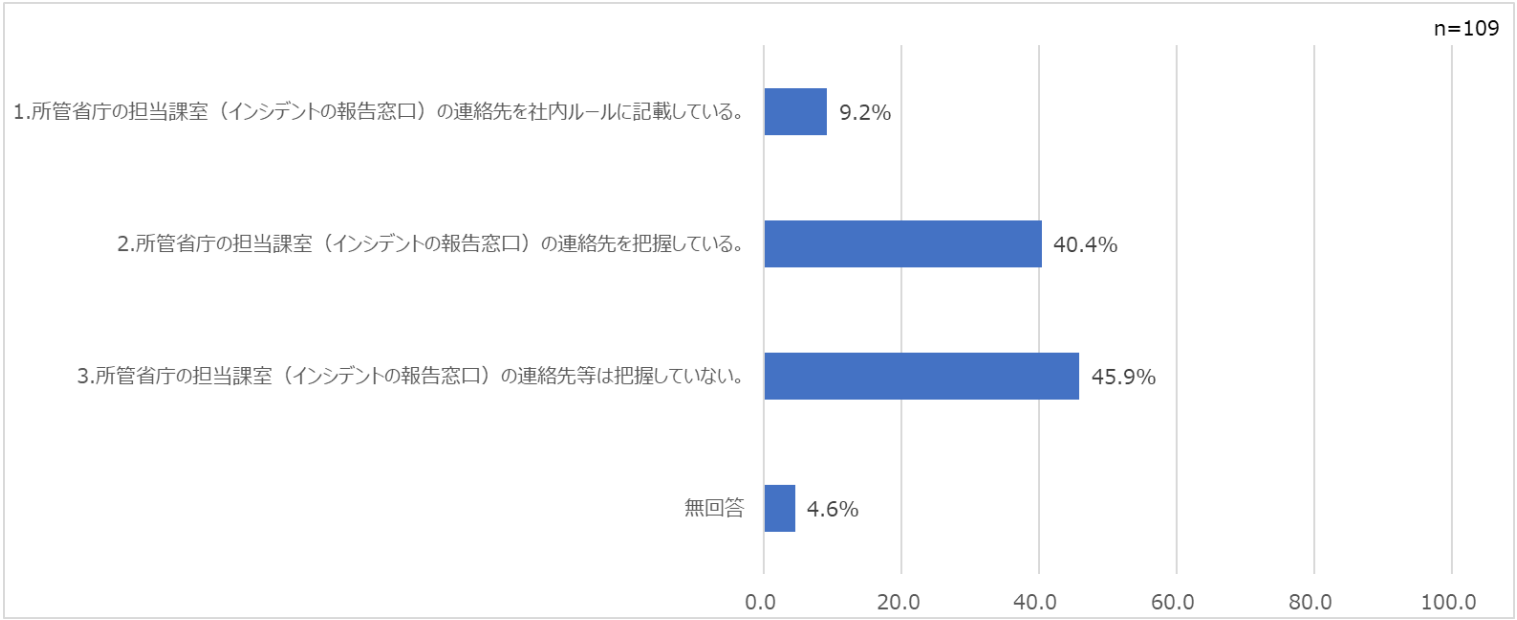
質問	貴社の制御システムインシデント対応体制は、制御システムインシデントに備えて各公的窓口とどのような日常の連携体制を構築しているか、その程度と併せてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：4-3-7

所管官庁の窓口との連携体制

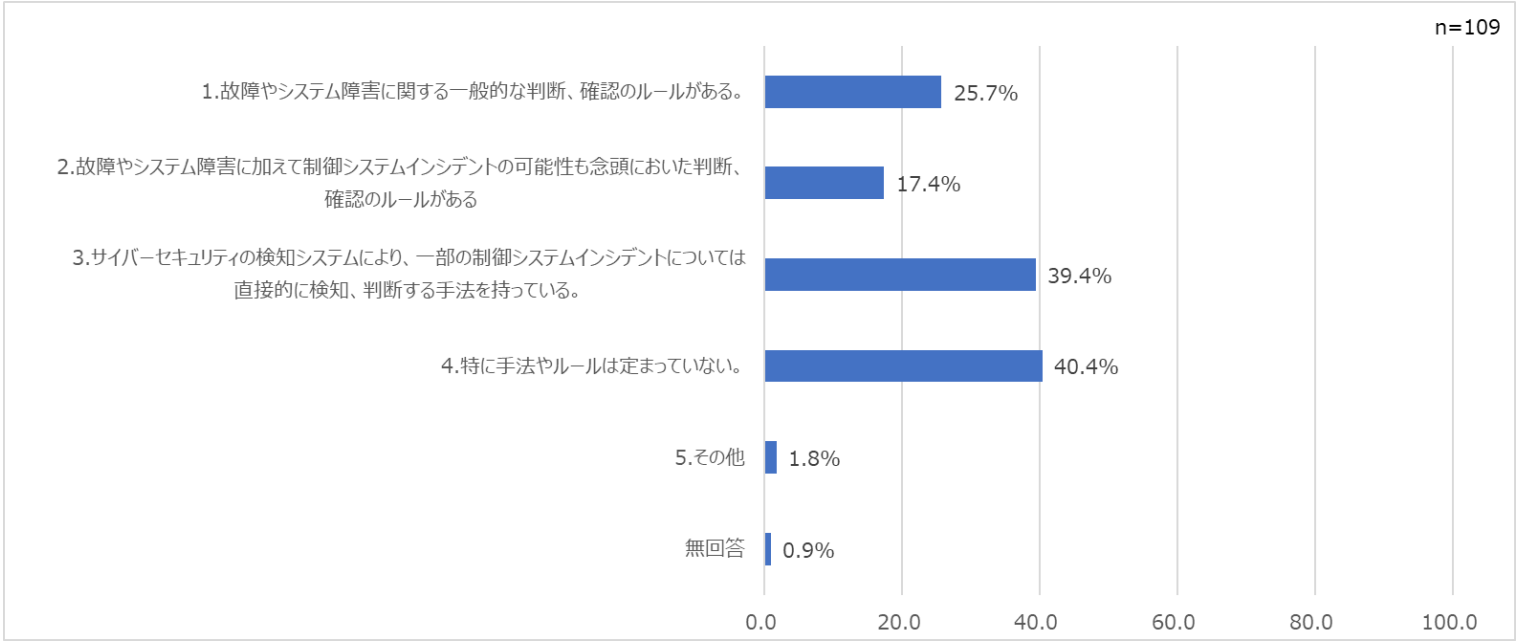
質問	貴社の制御システムインシデント対応体制は、制御システムインシデントに備えて各公的窓口とどのような日常の連携体制を構築しているか、その程度と併せてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：4-3-8

故障・障害の発生を認識するための方法に関する手法やルール（1/4）

質問	貴社では制御システムインシデントを含む機器やシステムの故障・障害の発生を認識するための方法について、何らかの手法やルールは定まっていますか。
回答形態	単一回答
自由記述欄	あり



設問番号：4-3-8

故障・障害の発生を認識するための方法に関する手法やルール（2/4）

選択肢の内容	個社の回答（自由記述）
故障やシステム障害に関する一般的な判断、確認のルールがある。（具体的に）	• クローズドネットワークで実施し、サーバはファイアーウォールにて防御。 • サービスによる監視、製造システム独自の監視機能によるアラート。 • ガイドライン。 • 各事業所の工務保全部門が対応し、必要に応じてシステムベンダーと連携して対処する。 • 各システムのエラーコードを記録・表示する機能があり、判断・確認が可能。 • 各装置の緊急時対策要領に定めている。 • 稼働監視ツール。 • 計装技術者の対応マニュアル等。 • 各生産技術部門にて判断・対応している。 • 基本的には制御システムに警報出力されるため、そのタイミングで故障、障害を認識している。 • 定めていない。 • 社則やガイドライン内で規定。 • 制御画面を確認することで正常に稼働しているか確認している。 • 生産設備の停止時間。 • 手順書。 • 日常点検。 • 日常点検・チェックシート。 • メーカーへの問い合わせ、社内ヘルプデスク窓口の設置。 • ユーザーからの通報。 • ログ、機器状態の確認にランプチェック。
故障やシステム障害に加えて制御システムインシデントの可能性も念頭においた判断、確認のルールがある（例えば、サイバーセキュリティ事象を念頭においたログ記録、データ収集等を行っている）。（具体的に）	• ファイアーウォールや主要なスイッチを通過する通信についてはログや通信そのもののデータを取得している。 • 一部の機器において、ログ記録・データ収集を行っている。 • 監査証跡の収集。 • 社則やガイドライン内で規定。 • 手順書。 • ネットワークの通信監視。 • ログの採取。 • ログ記録。 • ログ記録およびログ監視の実施。 • ログ収集は社内で範囲と期間を定めている。 • ログ保存。

設問番号：4-3-8

故障・障害の発生を認識するための方法に関する手法やルール（3/4）

選択肢の内容	個社の回答（自由記述）
サイバーセキュリティの検知システムにより、一部の制御システムインシデントについては直接的に検知、判断する手法を持っている。（具体的に）	• 振る舞い検知製品。 • EDR。 • EDRによる検知、SOCによる監視、CSIRTによる判断。 • 不正接続防止ツール。 • IPS、次世代ファイアーウォールの設置。 • 制御システムセキュリティサービス。 • 制御システムセキュリティサービスによる検知。 • UTMによる日常監視を実施。 • PC系設備は、スタンドアロンはUSBによるウィルスチェック、ネットワーク内は保護ソフトウェアを活用中。 • セキュリティツールによるチェック。 • 一部の制御システムでIDSを導入して運用を開始した。 • 一部の制御システムのみ、IT/OT境界ファイアーウォール（IDS）設置、Windows端末の防御ソフトを導入している。 • USBメモリ型ウィルス対策ソフト。 • 外部MSS（マネージドセキュリティサービス）による常時監視体制。 • 機器やシステムの死活監視とセキュリティ検知を実施。 • 工場ファイアーウォールでのIDS管理。 • サイバーセキュリティの検知システムにより、PC制御端末/制御機器/サーバの通信パケットを収集し、その振る舞い・挙動を検知している。 またユーザーヒアリングによって通常の状態であるかどうかを確認、判断する。 • システムにインストールしているウィルス対策ソフトと本社側からのアラート。 • 主要設備群単位でUTM設置等。 • 侵入検知装置。 • セキュリティソフトによる検知。 • ネットワークログの収集と監視の実施。 • ネットワーク監視、ファイアーウォールログ記録など。 • ネットワーク監視装置。 • ファイアウォールのログ監視及びIDSを利用している。 • ファイヤーウォールの監視。 • マルウェア対策ソフトが入っているシステムがある。IT-OT境界にUTMを設置している。

設問番号：4-3-8

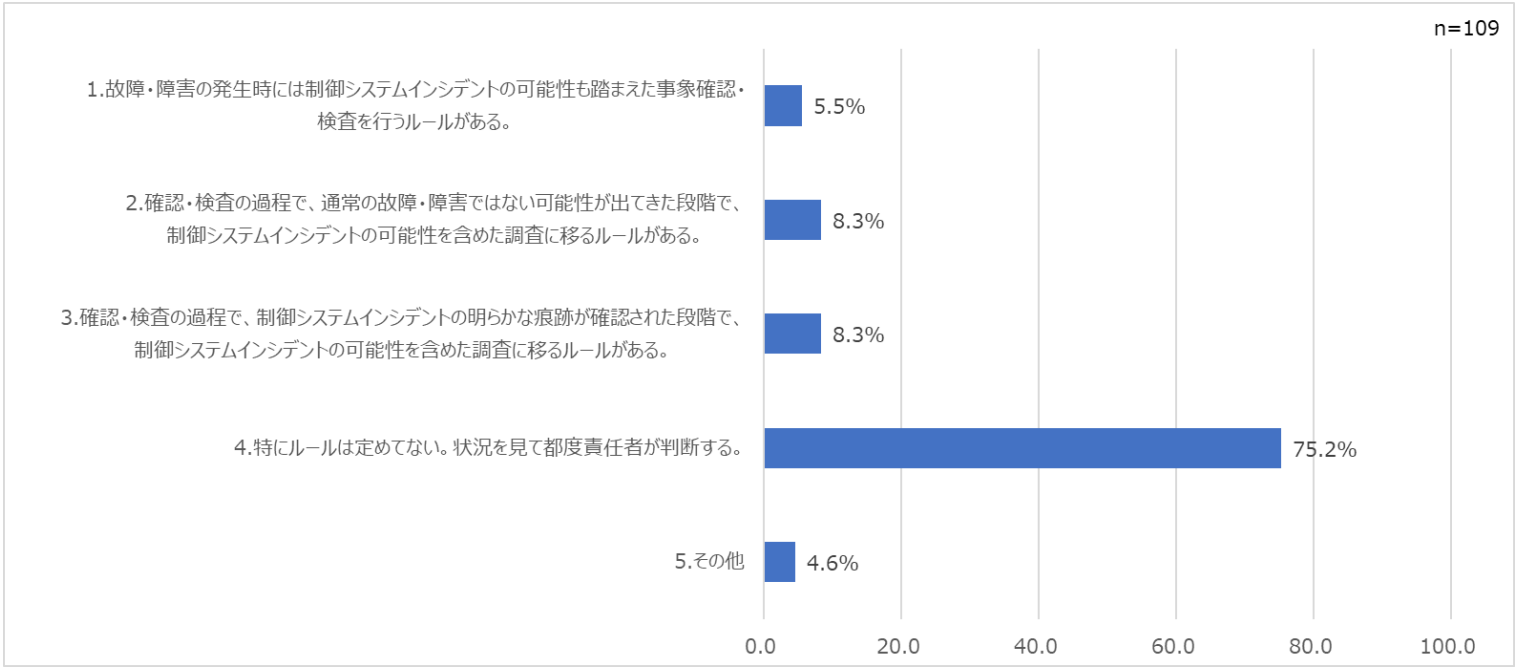
故障・障害の発生を認識するための方法に関する手法やルール（4/4）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• インシデントの検知については、IT-OTネットワークのファイアーウォールによる分離を推進しており、ファイアーウォールのログ監視を実施して、不正な通信がないか日次で確認をしている。 故障・障害の検知については、制御システムの故障・障害について仕組み化されておらず、設備作業員の現場確認による。 • 現状未定。 • 検討中。 • 工場のネットワークを対象としたサイバーセキュリティの検知システムを整備中である。 • 手法やルールは定まっていない。

設問番号：4-3-9

故障・障害と制御システムインシデントの切り分けに関する手法・ルール（1/2）

質問	貴社では機器やシステムの故障・障害と制御システムインシデントの切り分けについて、何らかの手法やルールは定まっていますか。
回答形態	複数回答
自由記述欄	あり



設問番号：4-3-9

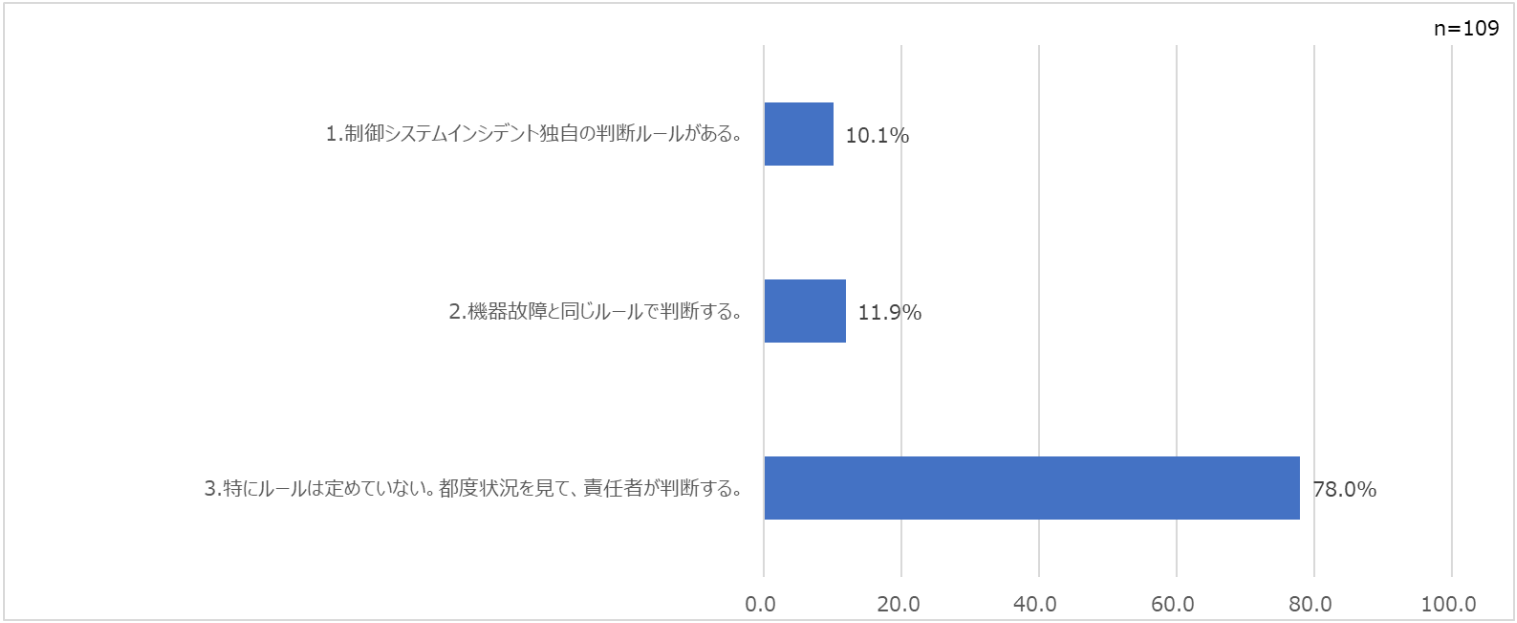
故障・障害と制御システムインシデントの切り分けに関する手法・ルール（2/2）

選択肢の内容	個社の回答（自由記述）
故障・障害の発生時には制御システムインシデントの可能性も踏まえた事象確認・検査を行うルールがある。（具体的に）	• CSIRTのPoCへ連絡報告するルールになっている。 • 基本的に制御システムでは個人情報や営業秘密とは分離されているため。NW追跡が可能な範囲での処理。 • 制御システムインシデントに関して要確認。
確認・検査の過程で、通常の故障・障害ではない可能性が出てきた段階で、制御システムインシデントの可能性を含めた調査に移るルールがある。（具体的に）	• CSIRTに通報してもらい対応に進む。 • 故障や障害の確認と同時にサイバー攻撃かを調査するルールとなっている。 • システムチェック。
確認・検査の過程で、制御システムインシデントの明らかな痕跡が確認された段階で、制御システムインシデントの可能性を含めた調査に移るルールがある。（具体的に）	• 運用ガイドライン。 • 脅迫画面が出る、マルウェア検知ソフトで検知など、明らかな痕跡があれば、調査に移る。 • 社内基準等。
その他（具体的に）	• 機器を扱うオペレータに対して故障と制御システムインシデントの切り分けをさせるルールに類するものはないが、SOCにより監視されているためインシデントの可能性があれば通知される仕組みになっている。 • 現在は、工場を管理する部門による判断であるが、工場のネットワークを対象としたサイバーセキュリティに関する規則、手順等を整備中である。 • 制御システムの故障や障害に対して手法やルールは特に定めていない。各制御システム担当部門に委ねられている。 サイバーインシデントの懸念がある場合は、全社ルールに則りエスカレーションされる。 • ルール化までは出来ていないが、通常の故障・障害ではない可能性としてセキュリティインシデントもありうることを教育・啓蒙し、相談・連絡できる部署を設けている。

設問番号：4-3-10

制御システムインシデント時の停止等の判断ルールについて（1/2）

質問	貴社では制御システムインシデント発生時の製造ライン停止等の判断ルールは定まっていますか。
回答形態	単一回答
自由記述欄	あり



設問番号：4-3-10

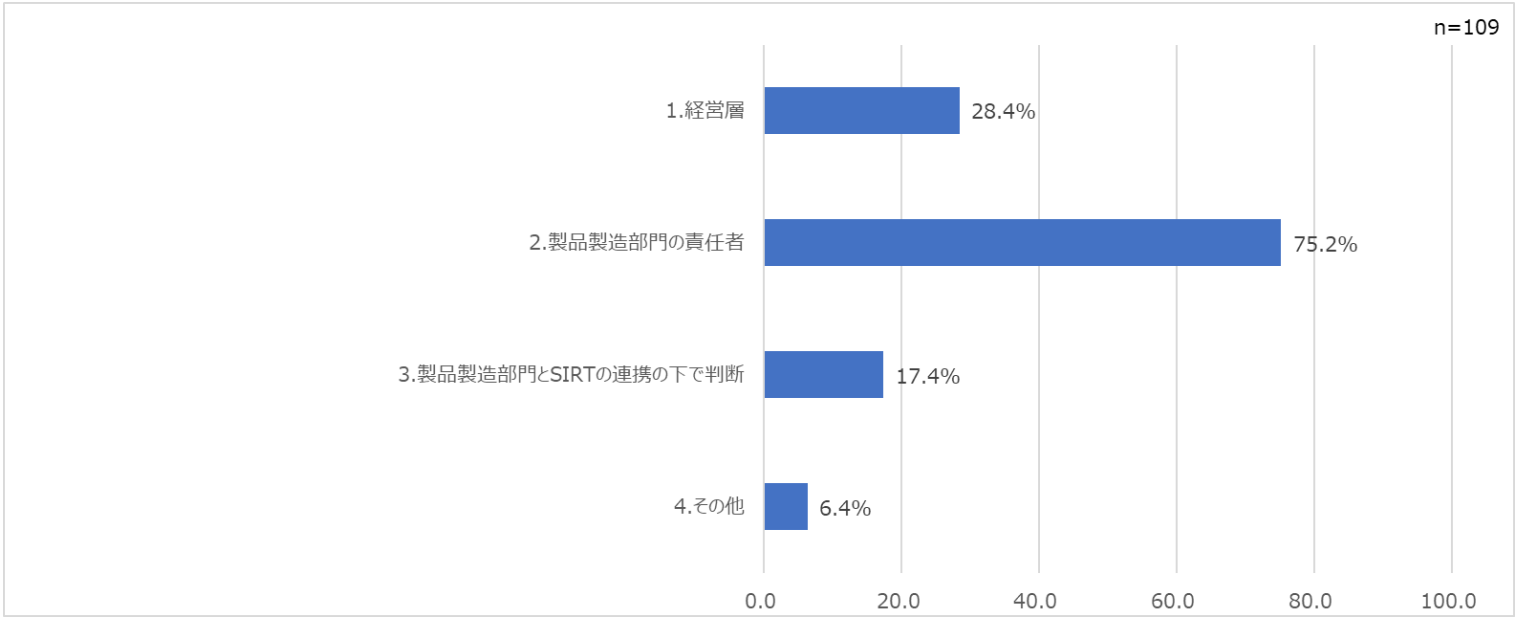
制御システムインシデント時の停止等の判断ルールについて（2/2）

選択肢の内容	個社の回答（自由記述）
制御システムインシデント独自の判断ルールがある。（具体的に）	• IT系のインシデント発生に関して、OTとのネットワーク分離を定めている。 • 感染確定時のネットワーク遮断、但しオフラインで可能な限り製造ライン継続。 • 社内基準等。 • 制御システムセキュリティインシデント対応ガイドラインを制定。 • 制御システムを含むセキュリティインシデント全般の対応ルールとして定めている。
機器故障と同じルールで判断する。（具体的に）	• エラー状況を確認し工程管理者の判断で実施。 • 緊急時対策要領で定めている。 • 部門長判断。

設問番号：4-3-11

制御システムインシデント時の停止等の判断者（1/2）

質問	貴社における制御システムインシデント発生時の製造ラインの停止等の判断者は誰ですか。
回答形態	複数回答
自由記述欄	あり



設問番号：4-3-11

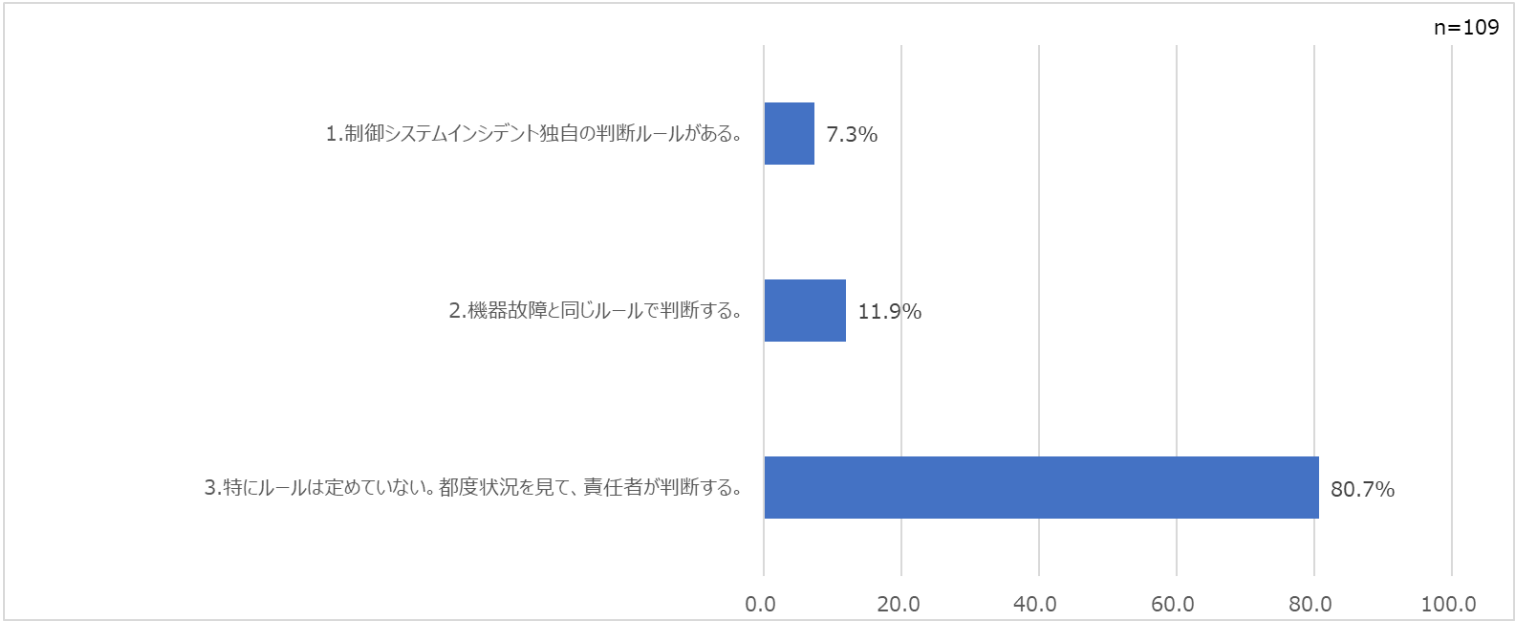
制御システムインシデント時の停止等の判断者（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 一般的には製品製造の責任者であるが、リスクの軽重に応じて判断基準が変わる。 • 製品供給先のグループ会社との協議にて決定する。 • 検討中。 • 工場長。 • 制御システム部門の責任者（サイバーセキュリティを統括している部門内の制御システムセキュリティ担当と相談することは可能）。 • 製造装置運転員。

設問番号：4-3-12

製造ライン復旧の判断に関するルール（1/2）

質問	貴社では制御システムインシデント発生時に、インシデントの収束を確認し、製造ラインの復旧等を行う判断ルールは定まっていますか。
回答形態	単一回答
自由記述欄	あり



設問番号：4-3-12

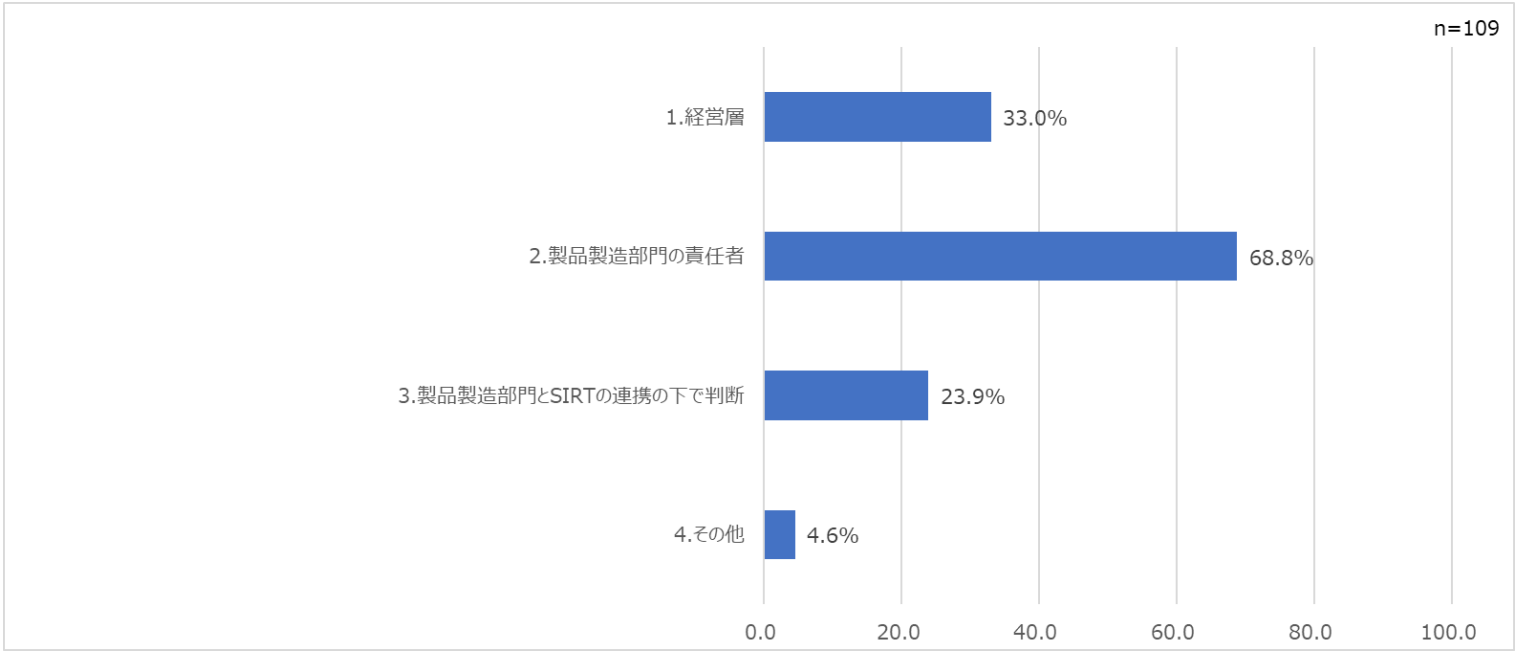
製造ライン復旧の判断に関するルール（2/2）

選択肢の内容	個社の回答（自由記述）
制御システムインシデント独自の判断ルールがある。（具体的に）	• エンタープライズ領域と同様（経営者の判断）。 • ガイドライン。 • 社内基準等。 • 制御システムを含むセキュリティインシデント対応ルールで定めている。
機器故障と同じルールで判断する。（具体的に）	• 当該装置の責任者。

設問番号：4-3-13

制御システムインシデント時の復旧等の判断者（1/2）

質問	貴社における制御システムインシデントの収束に当たっての、製造ラインの復旧等の判断者は誰ですか。
回答形態	複数回答
自由記述欄	あり



設問番号：4-3-13

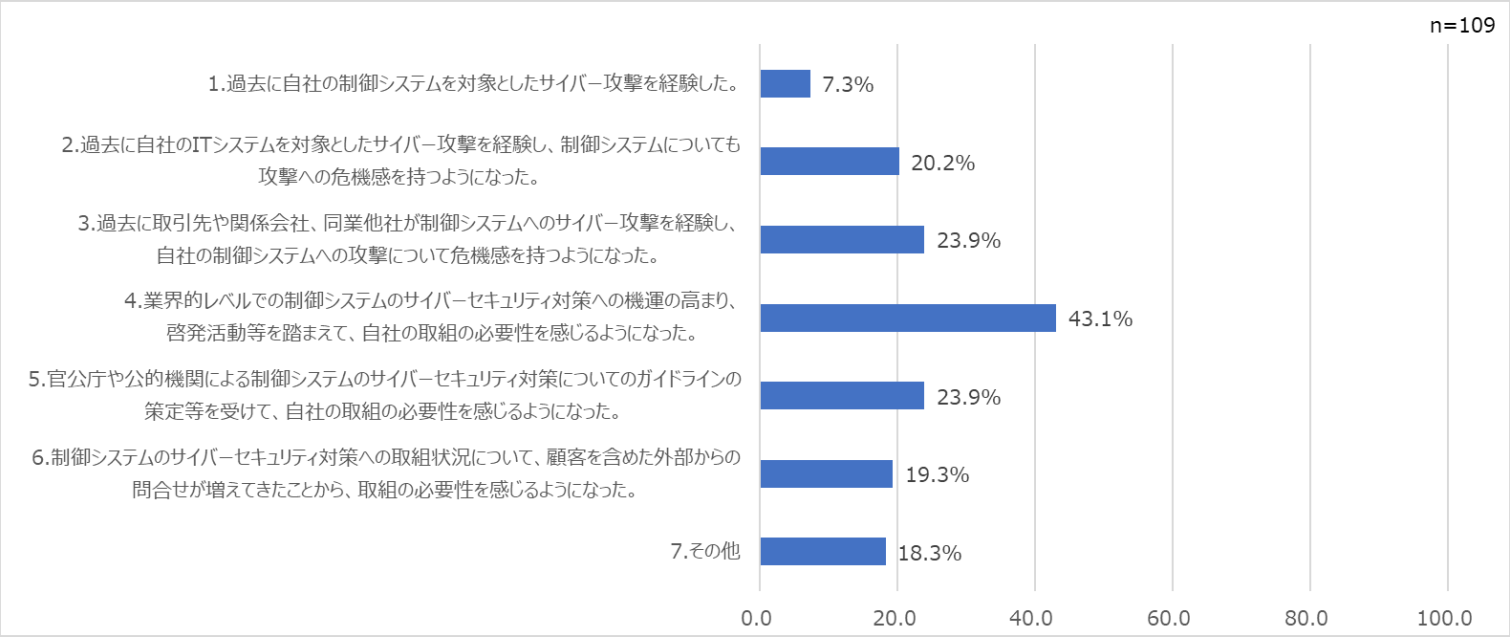
制御システムインシデント時の復旧等の判断者（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 一般的には製品製造の責任者であるが、リスクの軽重に応じて判断基準が変わる。 • 検討中。 • 現状は決まっていない。 • 制御システム部門の責任者がサイバーセキュリティを統括している部門内の制御システムセキュリティ担当と連携の下で判断。 • 製造部門の長。

設問番号：4-4-1

制御システムインシデント対応体制の組織化の背景（1/2）

質問	貴社において制御システムインシデント対応体制を組織したきっかけや背景について近いものをお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：4-4-1

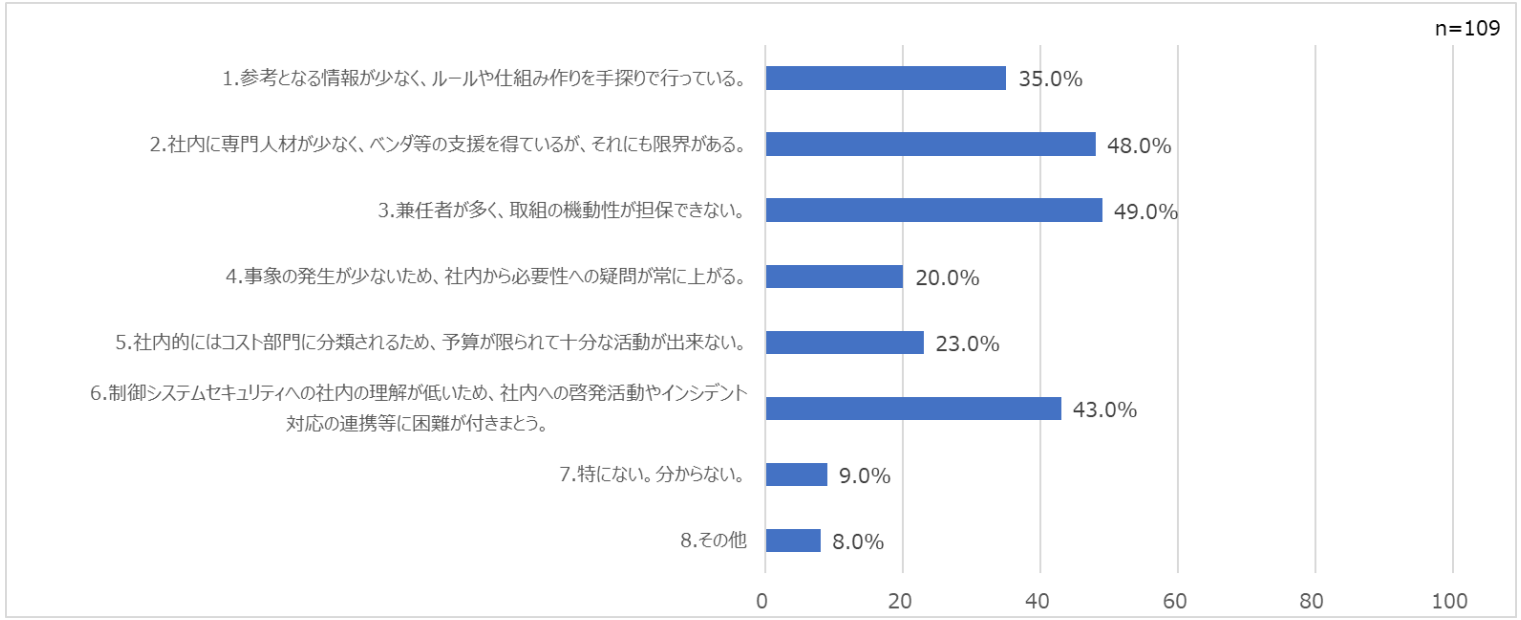
制御システムインシデント対応体制の組織化の背景（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 一般IT機器と同じ管理をしている。 • 親会社からの指示に基づく。 • 親会社からの制御システムセキュリティ対策の要請による。 • 親会社要求。 • 機運の高まりを受けて必要性は感じるが、組織まではできていない。 • 旧親会社からの要請。 • 現状未整備であったことから。 • 検討していない。 • 事業関連法改正への対応。 • 今後検討課題。 • 制御システムに関しての対応体制は構築されていない。 • 制御システムに特化した対応体制は無い。 • 全社のセキュリティ担当部門があるだけで個別に組織されていない。 • 体制を検討中。 • 特定のきっかけはない。 • まだ組織されていない。 • 特に無し、通常の体制で対応。

設問番号：4-4-2

制御システムインシデント対応体制の組織的課題（1/2）

質問	貴社における制御システムインシデント対応体制の取組に関して、組織的課題や改善が必要な点についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：4-4-2

制御システムインシデント対応体制の組織的課題（2/2）

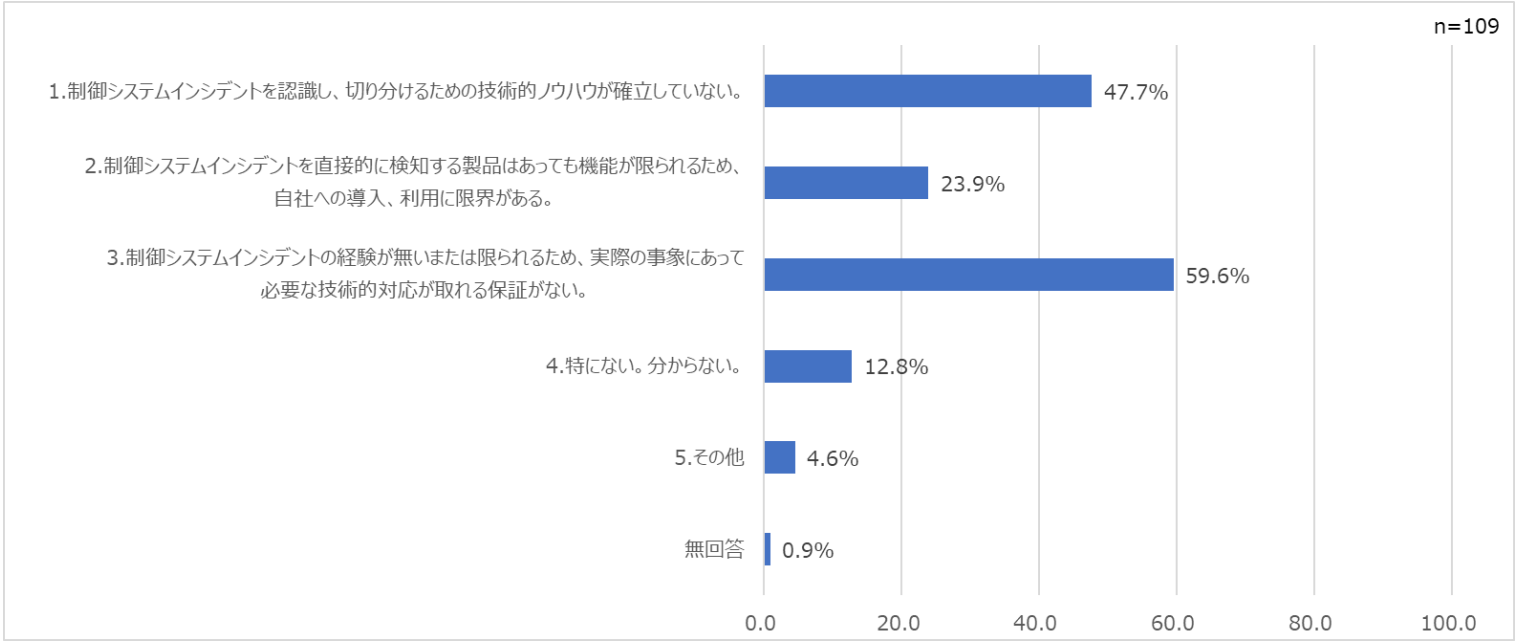
選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 1から6全部経営者の危機感が薄く、ミドルアップでの活動になっている。 • システム間の連携等が多く、またIT/OTの所掌やシステム子会社の立ち位置・ファシリティ面の問題などもあるため、ルール策定等が難しい。 • コストとリスクの比較が難しく、投資の判断が難しい。 • 制御システム特有の課題の対処。 • 制御系向けの対策体制はない。 • 生産拠点ごとに特徴があることや、生産活動にも影響が出る可能性があるため、一般的なルールを社内に単純に適用させることは難しく、各拠点と協力しながら当社にあった対策・ルールを検討・適用していく必要があり、時間がかかる。 • 対策は費用対効果となるため現実的でない。 • ルールづくりのための情報は豊富にあると思っているが、兼任者のみのため、歩みが遅い。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：4-4-3

制御システムインシデント対応体制の技術的課題（1/2）

質問	貴社における制御システムインシデント対応体制の取組に関して、技術的課題や改善が必要な点についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：4-4-3

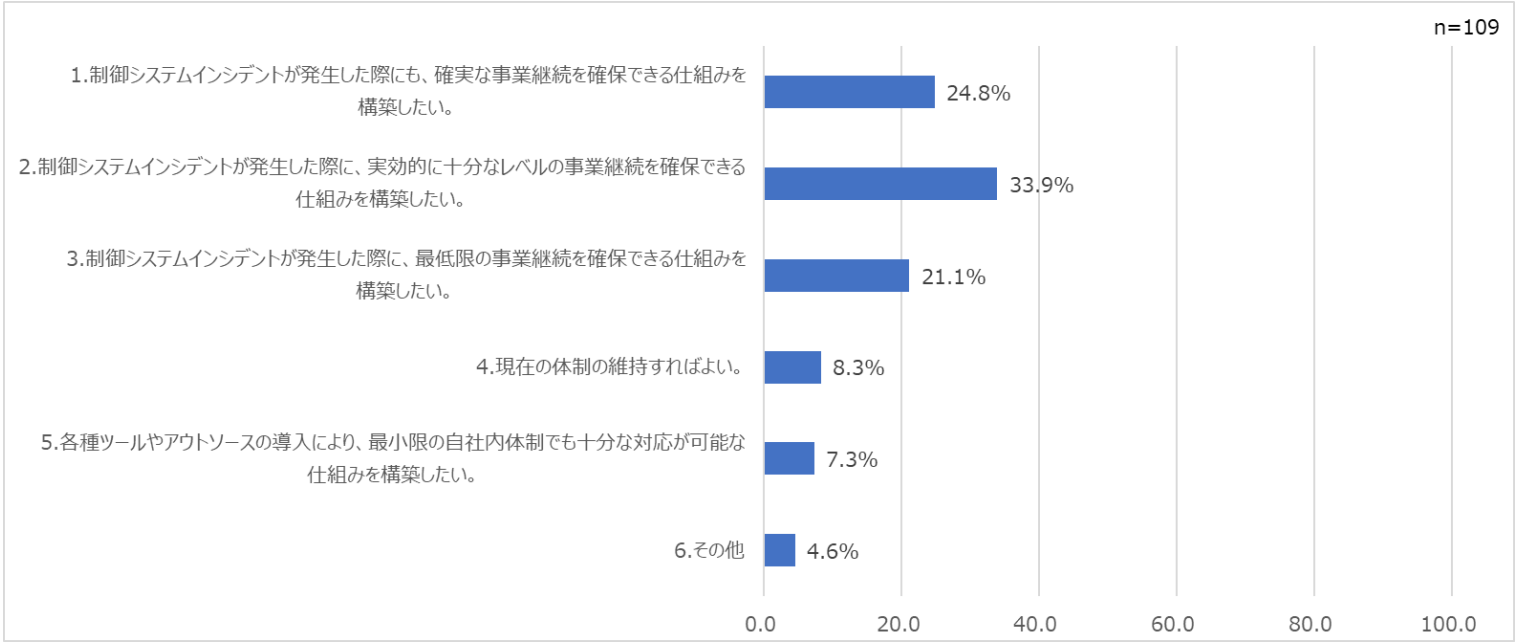
制御システムインシデント対応体制の技術的課題（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 一時対応を行うのは保守部門のため、システムに対する知識が乏しい。 • 検知、監視システムが制御システムの動作に影響を与えるか否かの検証が困難。 • 制御システムに特化した技術的対策の導入。 • 制御ベンダのサポートが得られなくなることや制御機器の制約で適用できない対策もある。 • 設備の構成上対応製品が利用不可の場合がある。 • 全制御システムにセキュリティ対応を行うには費用と年月がかかりすぎる。制御システムベンダー側の対応が会社により大きな差がある。 • 対象設備が多く、対策に多くの費用が必要。

設問番号：4-4-4

制御システムインシデント対応体制の活動の目標、将来像（1/2）

質問	貴社における制御システムインシデント対応体制の活動の目標や将来像等についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：4-4-4

制御システムインシデント対応体制の活動の目標、将来像（2/2）

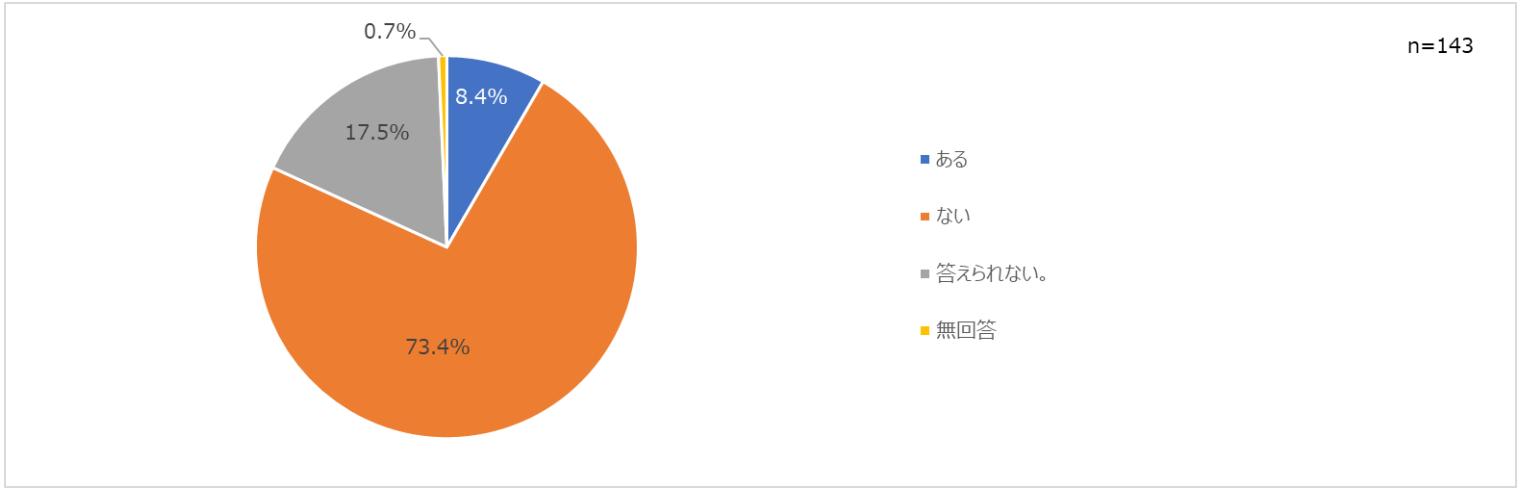
選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 選択肢2、3のいずれか。 • 検討中。 • 制御システムインシデントが発生した際に、実効的に十分なレベルの事業継続を確保できる仕組みを、各種ツールやアウトソースの導入により、最小の自社内体制で構築したい。 • 制御システムに特化した対応体制は無い。 • 必要性について検討されていない。

※上記「個社の回答（自由記述）」欄における数字は、前頁における回答選択肢の番号を示している。

設問番号：5-1-1

インシデント発生事例（1/2）

質問	過去に制御システムインシデントが発生した経験はありますか。ある場合は、過去5年間（2019年～2023年）の発生頻度はどのくらいですか。
回答形態	単一回答
自由記述欄	あり



設問番号：5-1-1

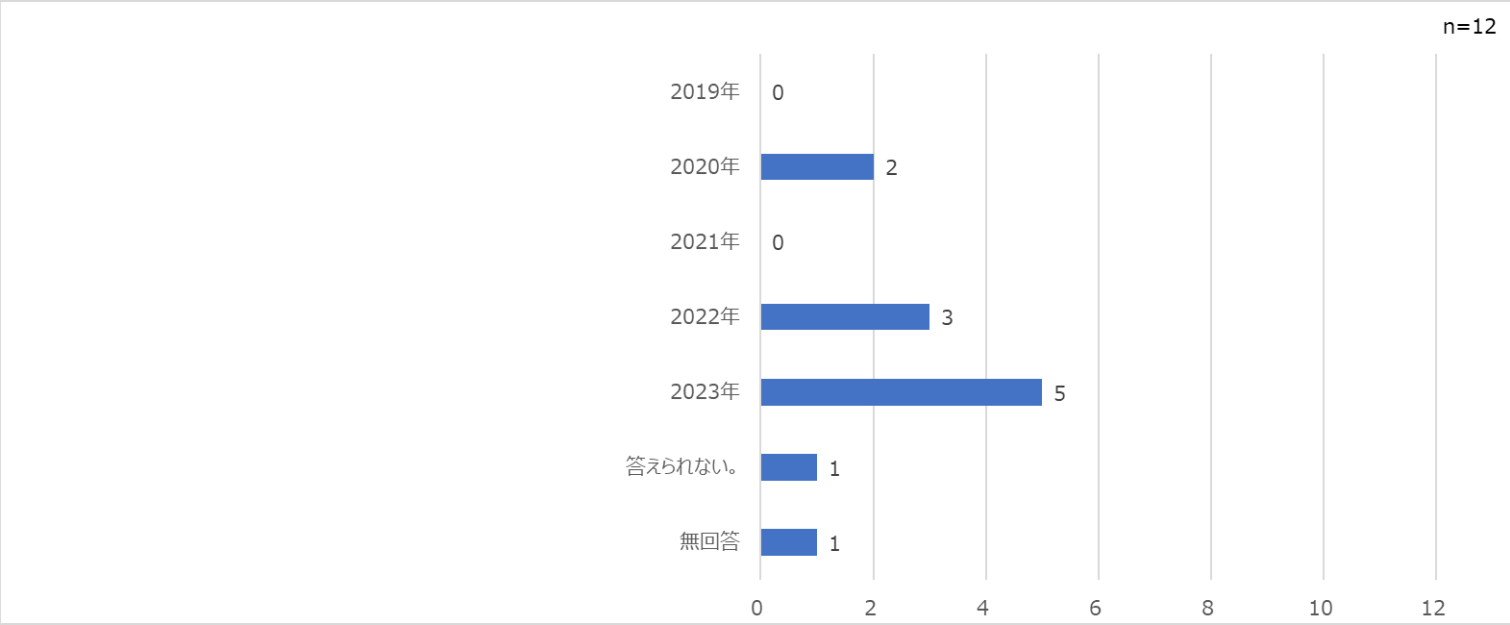
インシデント発生事例（2/2）

選択肢の内容	個社の回答（自由記述）
ある場合の発生頻度（具体的に）	• 1回 • 1回 • 1回 • 1回 • 1回 • 1回 • 1回 • 2回 • 10回

設問番号：5-2-1

制御システムインシデントが発生した時期

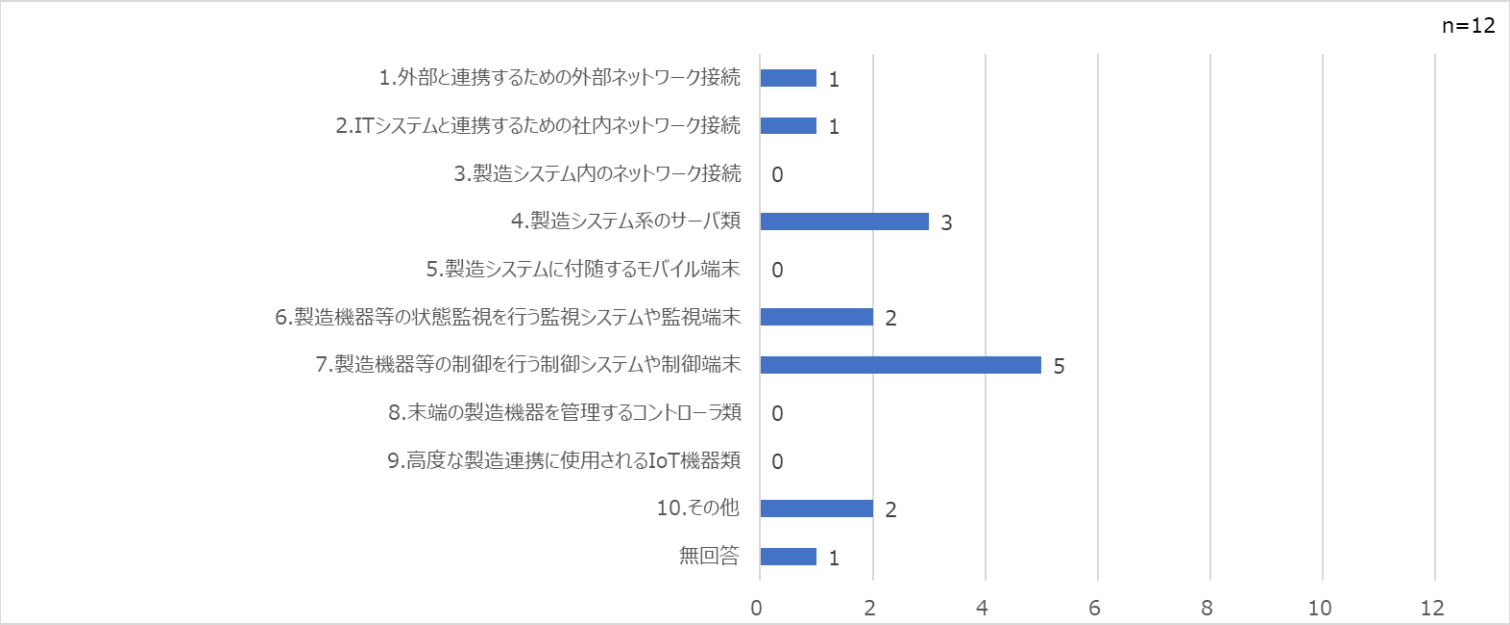
質問	その制御システムインシデントが発生した時期についてお答えください。
回答形態	複数回答
自由記述欄	なし



設問番号：5-2-2

被害を受けたシステム、製造制御システム（1/2）

質問	その制御システムインシデントに関して、被害を受けたシステム、製造制御システムについてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-2-2

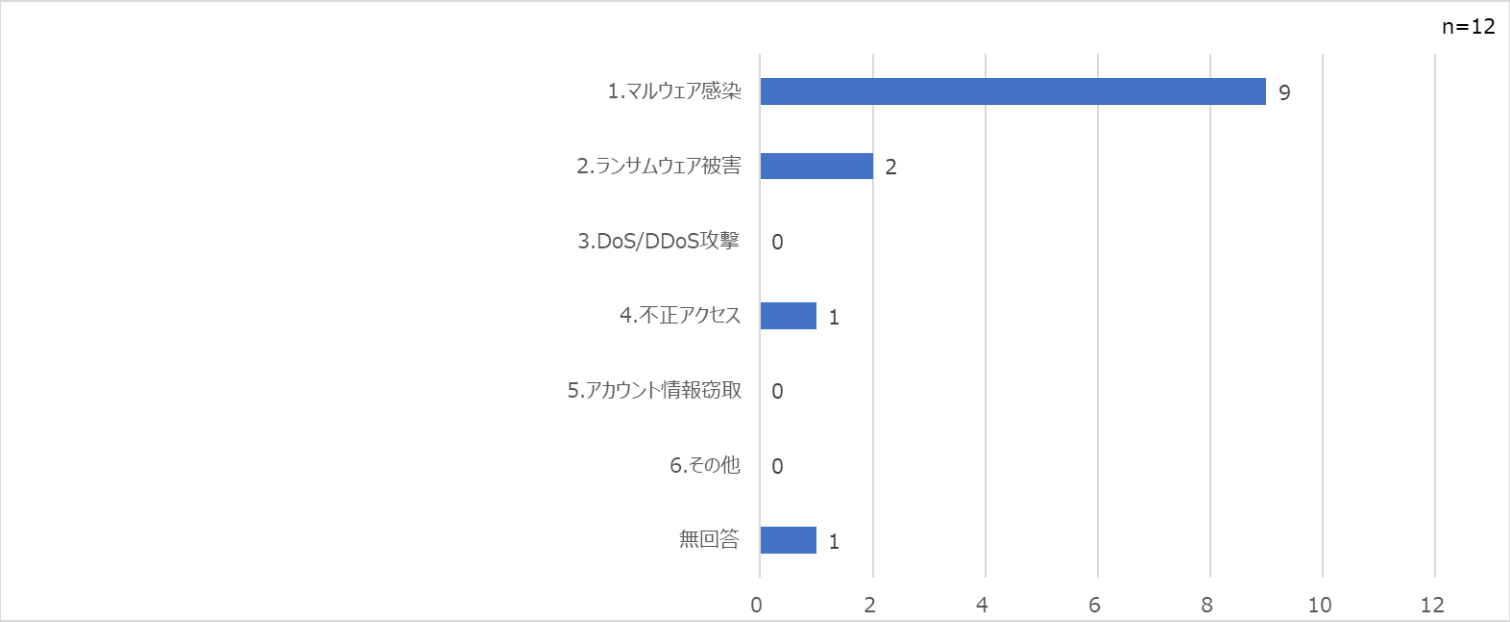
被害を受けたシステム、製造制御システム（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• スタンドアロンのPC系製造設備。

設問番号：5-2-3

システムに対する攻撃（1/2）

質問	その制御システムインシデントに関して、システムに対する攻撃は次のどれに近いものかお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-2-3

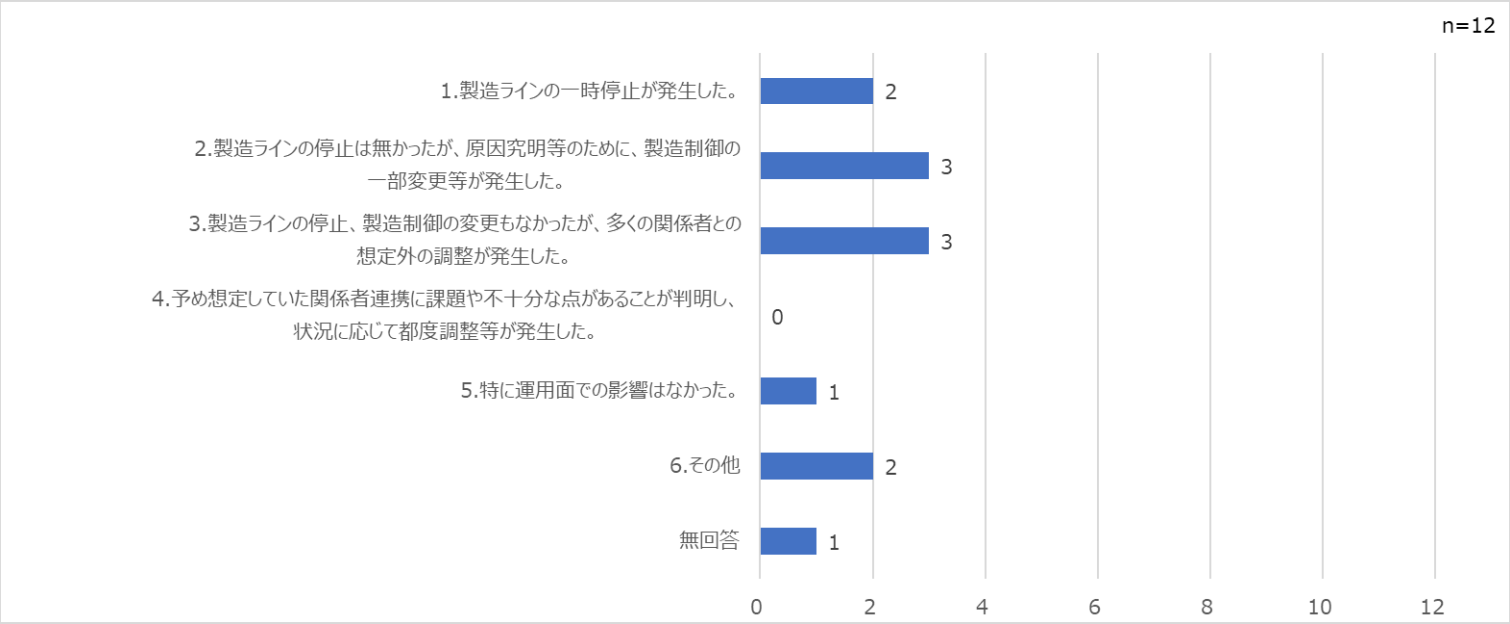
システムに対する攻撃（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 使用ソフトの利用期限が変更され、再度のインストールが必要になる。

設問番号：5-2-4

インシデントの製造システムの運用面への影響（1/2）

質問	その制御システムインシデントに関して、システムが被害を受けた結果として、製造システムの運用面にどのような影響が出たかお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-2-4

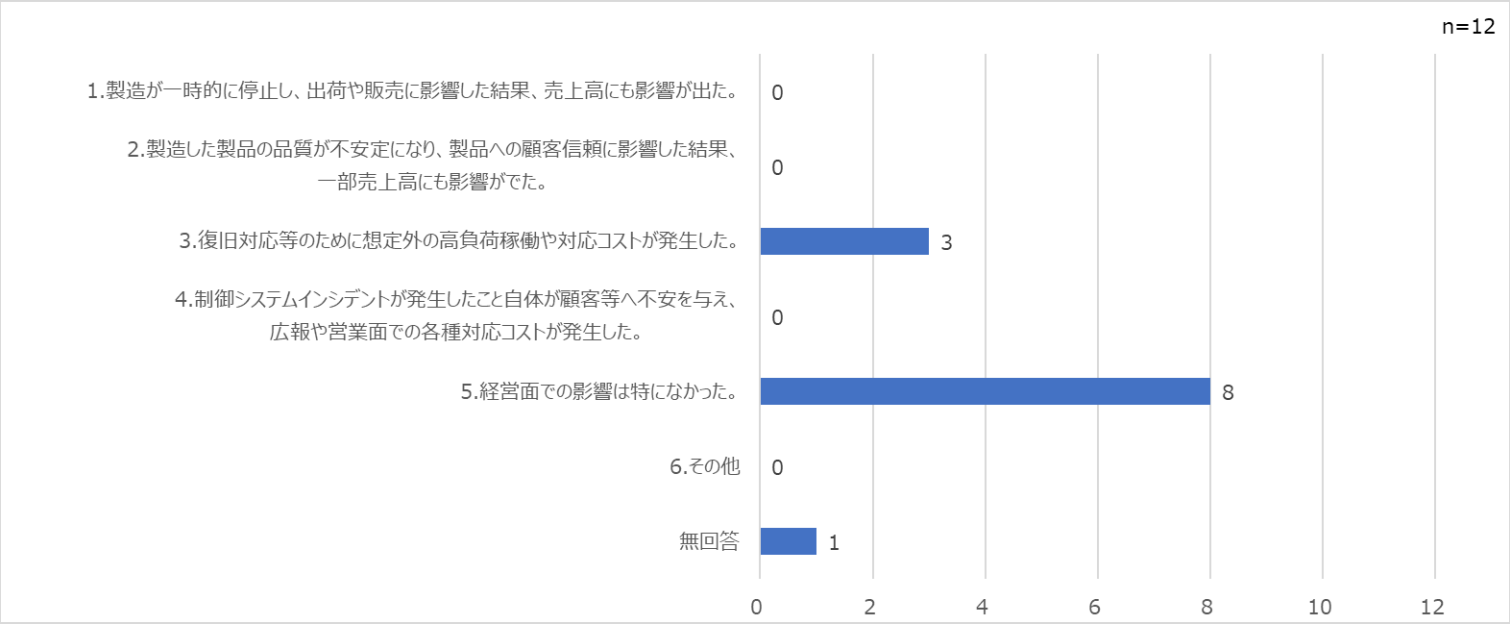
インシデントの製造システムの運用面への影響（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 一部の故障を検知してメールを送付する仕組みを一時的に停止させた。 • 再インストールで使用可能になったが、海外製セキュリティソフトとの兼ね合いで使用不可になるので、セキュリティソフトの変更をした。 • 製造ライン停止、製造製品へのマルウェア混入。

設問番号：5-2-5

インシデントの経営面への影響（1/2）

質問	その制御システムインシデントに関して、システム被害や製造システムの運用面への影響の結果として、経営面にどのような影響が出たかお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-2-5

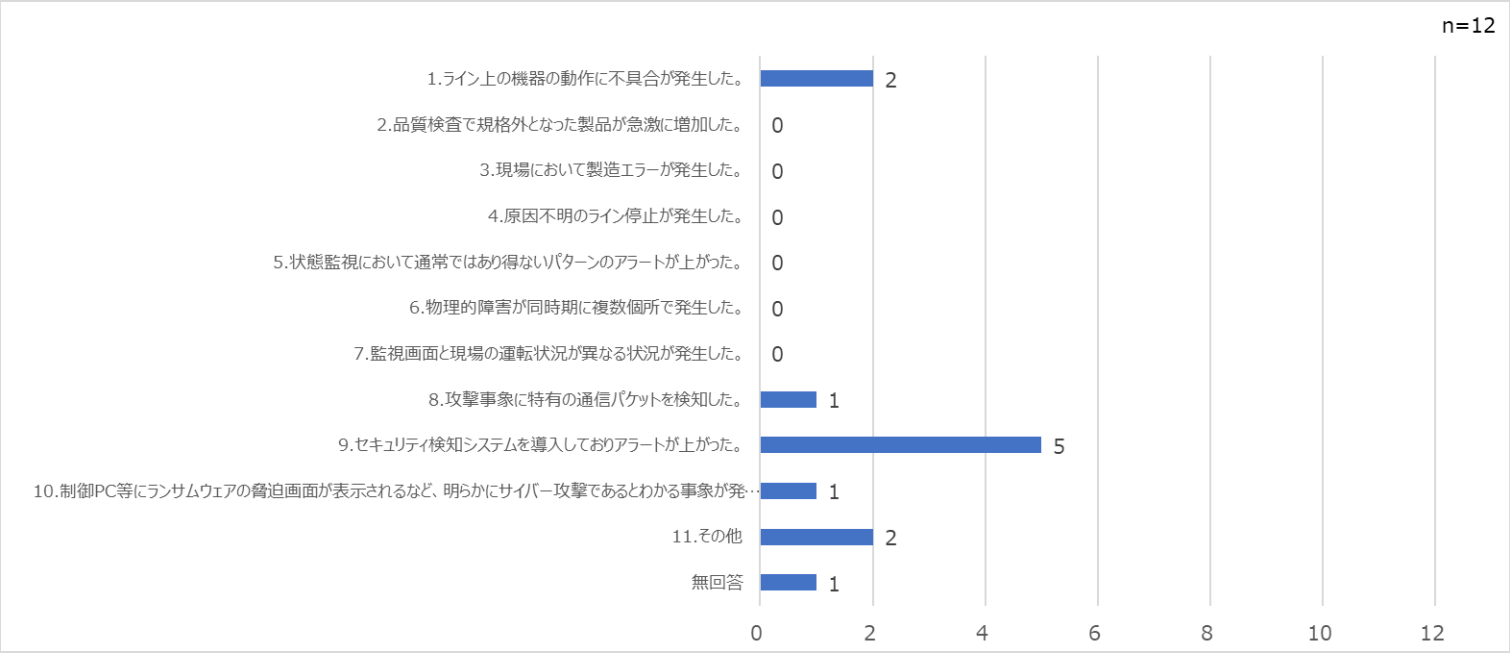
インシデントの経営面への影響（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 2～3日の休止で特に影響はない。

設問番号：5-3-1

制御システムインシデントを把握したきっかけ（1/2）

質問	その制御システムインシデントを最初に把握（当初、故障・障害と認識されていた場合はその故障・障害の把握時点）したきっかけとなった事象についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-3-1

制御システムインシデントを把握したきっかけ（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 一部機能が使用不可。 • 外部との通信量が増加し、通信料が跳ね上がった。

設問番号：5-3-2

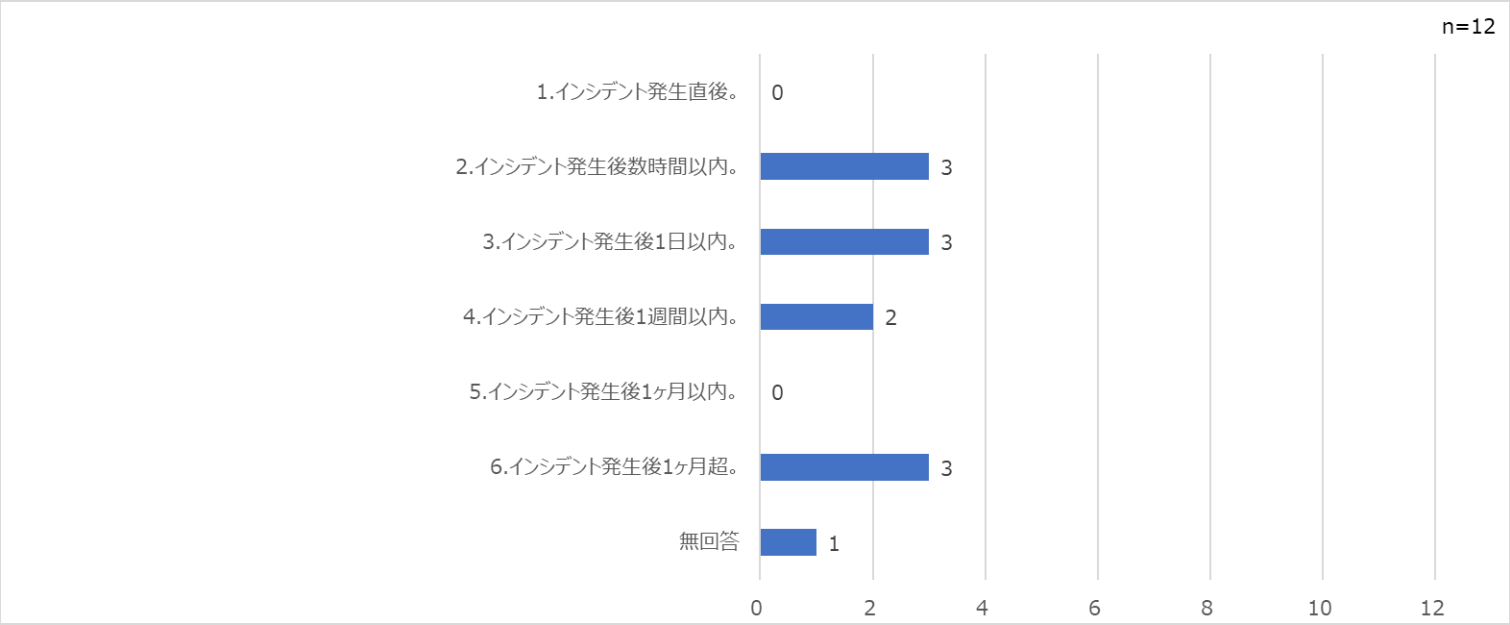
制御システムインシデントの第一発見者（設問番号：5-3-1の事象を発見した人）の所属や属性等

質問	その制御システムインシデントの第一発見者（設問番号：5-3-1の事象を発見した人）の所属や属性等についてお答えください。
回答形態	自由記述
回答数	11
個社回答	• CSIRT。 • IT子会社　セキュリティ監視担当。 • SOCベンダー。 • ウィルス検査実施者(工場の制御系システム担当者)。 • 使用者。 • 生産管理グループ。 • 海外工場生産技術部門。 • 情報システム部でEDRを制御系端末に展開している最中にマルウェアを検知した。 • 情報セキュリティ部。 • 対象機械作業員。 • 通信量の支払いを行っている情報システム部門。

設問番号：5-3-3

制御システムインシデントがサイバー攻撃によるものと把握した時期

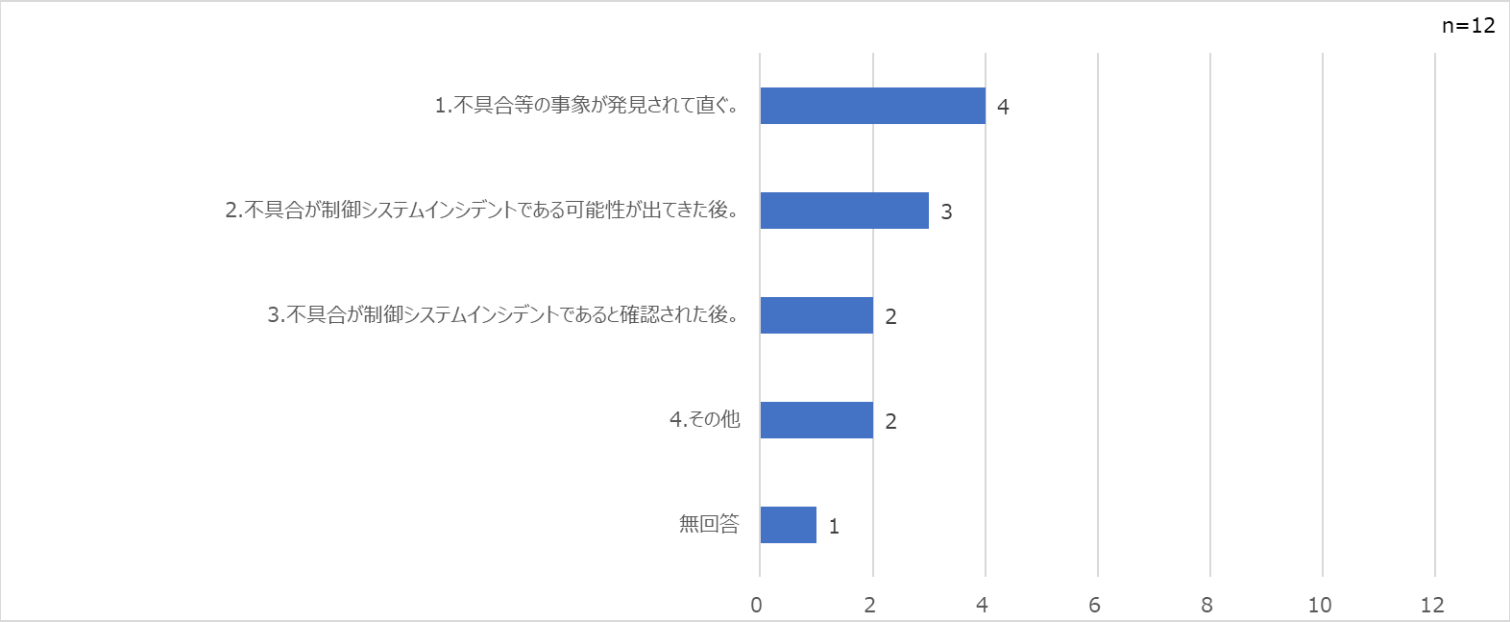
質問	その制御システムインシデントがサイバー攻撃による制御システムインシデントであると把握した時期についてお答えください。
回答形態	単一回答
自由記述欄	なし



設問番号：5-3-4

制御システムインシデント対応体制が報告を受けたタイミング（1/2）

質問	その制御システムインシデントに関して、制御システムインシデント対応体制が報告を受けたタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-4

制御システムインシデント対応体制が報告を受けたタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• EDRを導入したタイミング。マルウェア感染時期は不明。 • ITのアラートとして、調査を開始した結果、発信元が制御システムの機器であることが判明した。 • 確認後、再インストールを2回行った後、セキュリティソフトのアンインストール。

設問番号：5-3-5

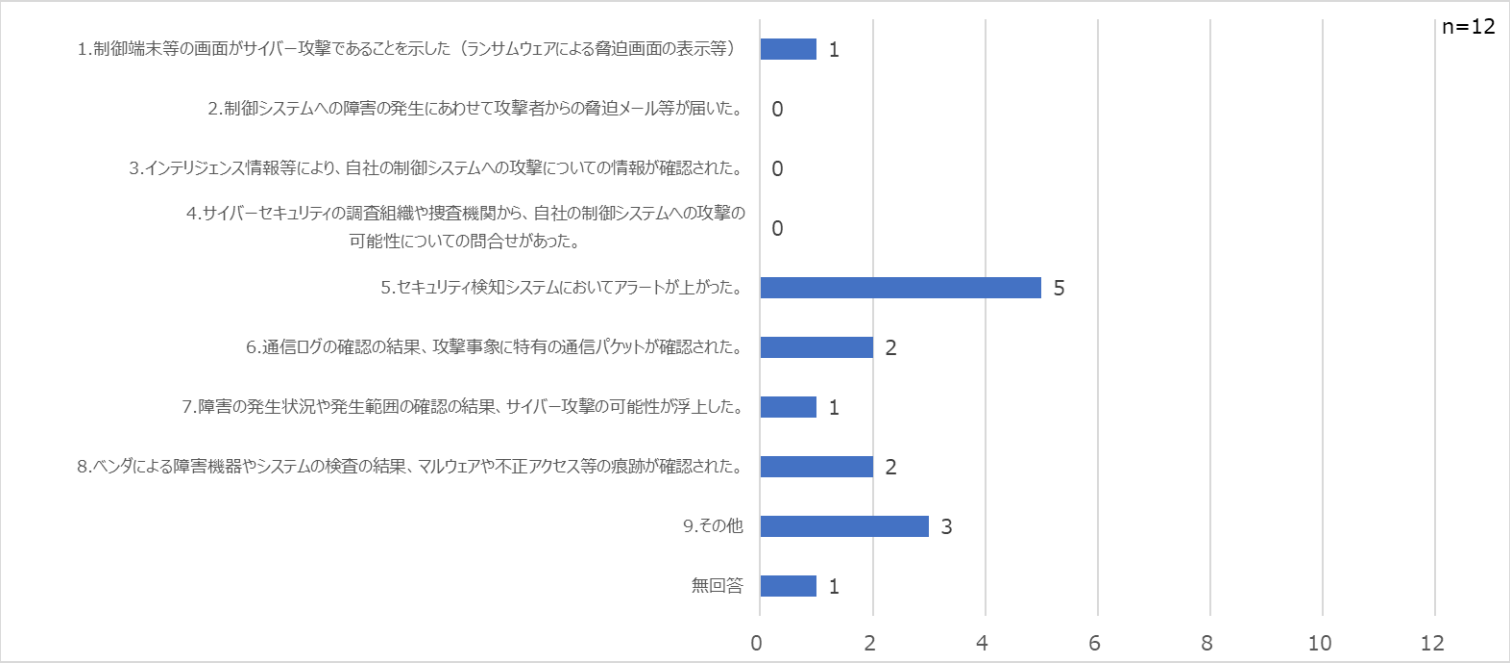
制御システムインシデント対応体制に報告した人の所属や属性等

質問	その制御システムインシデントに関して、制御システムインシデント対応体制に報告した人の所属や属性等についてお答えください。
回答形態	自由記述
回答数	11
個社回答	• CSIRT。 • SOCベンダー。 • 現場のセキュリティ責任者。 • 上司に報告、上司の指示で、情報システムに報告。 • 情報管理グループ。 • 情報システム部。 • 情報セキュリティ部。 • 制御システムを保有するグループ会社のIT担当者。 • 製造システム管理部門→情報システム部門→制御システムセキュリティ部門。 • 製造現場。 • 体制は検討中 関係者に報告した人は、海外工場の開発窓口担当。

設問番号：5-3-6

制御システムインシデントがサイバー攻撃によるものと確認・判断した方法（1/2）

質問	その制御システムインシデントに関して、不具合の原因が機器やシステムの単なる故障や障害ではなく、サイバー攻撃による制御システムインシデントであると確認、判断した方法についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-3-6

制御システムインシデントがサイバー攻撃によるものと確認・判断した方法（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 選択肢8：自社の検査で発見。 • ウィルス付きUSB。 • エクセルファイルが脅迫文のテキストファイルに置き換えられていた。 • ベンダーから海外製のセキュリティソフトに起因するインシデントとの報告を受けて、対応を行う。

設問番号：5-3-7

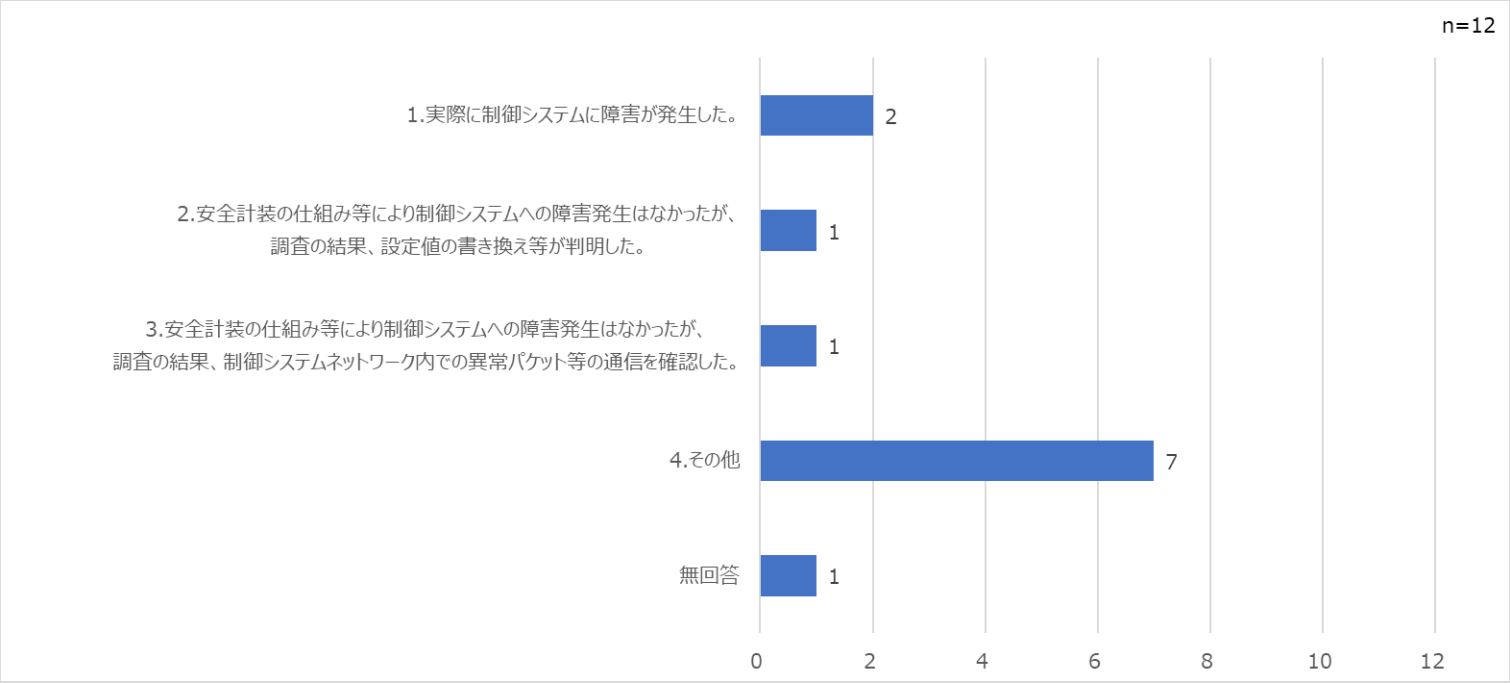
制御システムインシデントがサイバー攻撃によるものと確認、判断した判断者の所属や属性等

質問	その制御システムインシデントに関して、不具合の原因が機器やシステムの単なる故障や障害ではなく、サイバー攻撃による制御システムインシデントであると確認、判断した判断者の所属や属性等についてお答えください。
回答形態	自由記述
回答数	11
個社回答	• CSIRT。 • IT子会社　セキュリティ監視担当。 • SOCベンダー。 • 一報を受けた情報セキュリティ部門の責任者。 • 海外工場の生産技術部門。設備トラブルといった事象として表れていたわけではなく、検査時にマルウェアが見つかったため、設備トラブルとの切り分け判断は必要なかった。 • 該当機器を管理している拠点の情報システム担当者。 • 現場のセキュリティ責任者。 • 情報管理グループ。 • 情報システム部EDR展開部署。 • 情報セキュリティ部CSIRT。 • ベンダーへ報告して、判断する。

設問番号：5-3-8

制御システムにおけるインシデントであると確認・判断した方法（1/2）

質問	その制御システムインシデントに関して、不具合の原因が情報系システムへのインシデント（マルウェア感染等）ではなく、制御システムへのインシデントであると確認、判断した方法についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-3-8

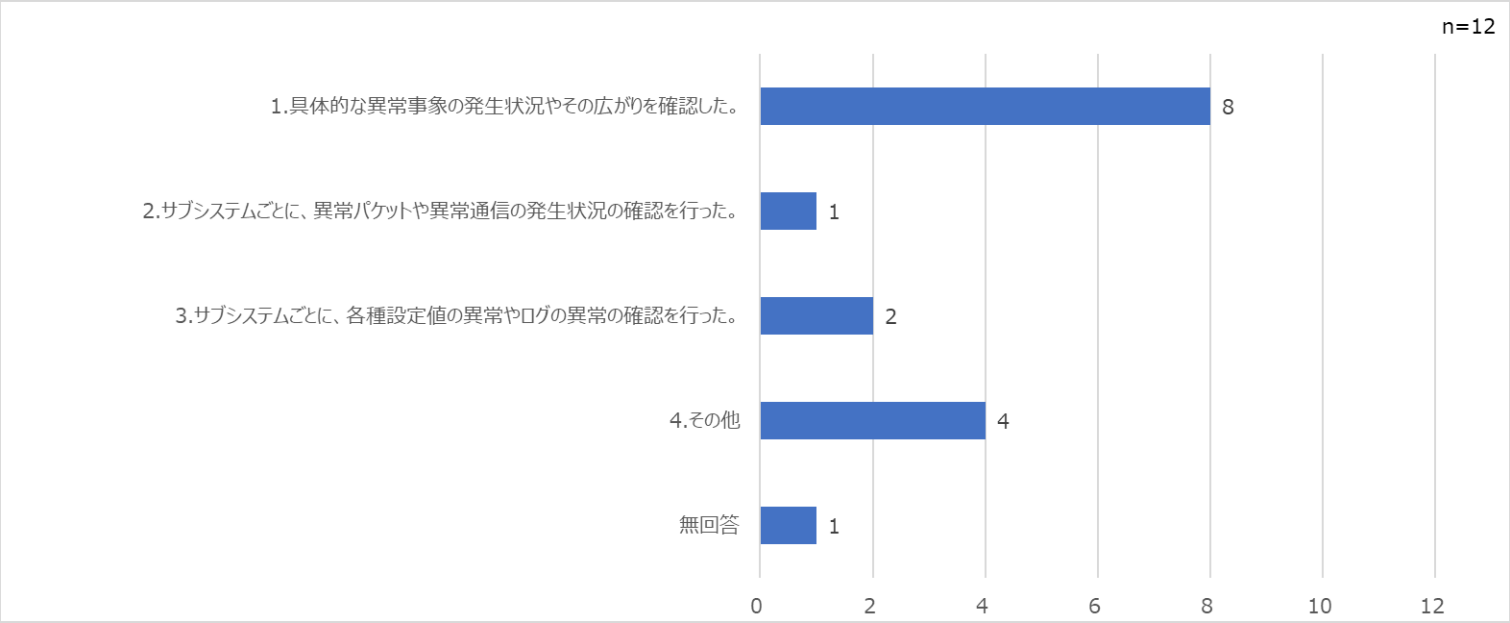
制御システムにおけるインシデントであると確認・判断した方法（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• IT系システムへの不審通信を検知し、通信元が制御系システムであった。 • USBにウィルス存在。 • 社内の情報系システムに接続のない制御システムであったため。 • 制御系NWの接続される端末でのマルウェア検知。 • 制御システムに障害発生。 • 通信パケットの発信元が制御システムであった。 • マルウェアが見つかったため。

設問番号：5-3-9

制御システムインシデントの影響範囲の確認方法（1/2）

質問	その制御システムインシデントの影響範囲の確認の方法についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-3-9

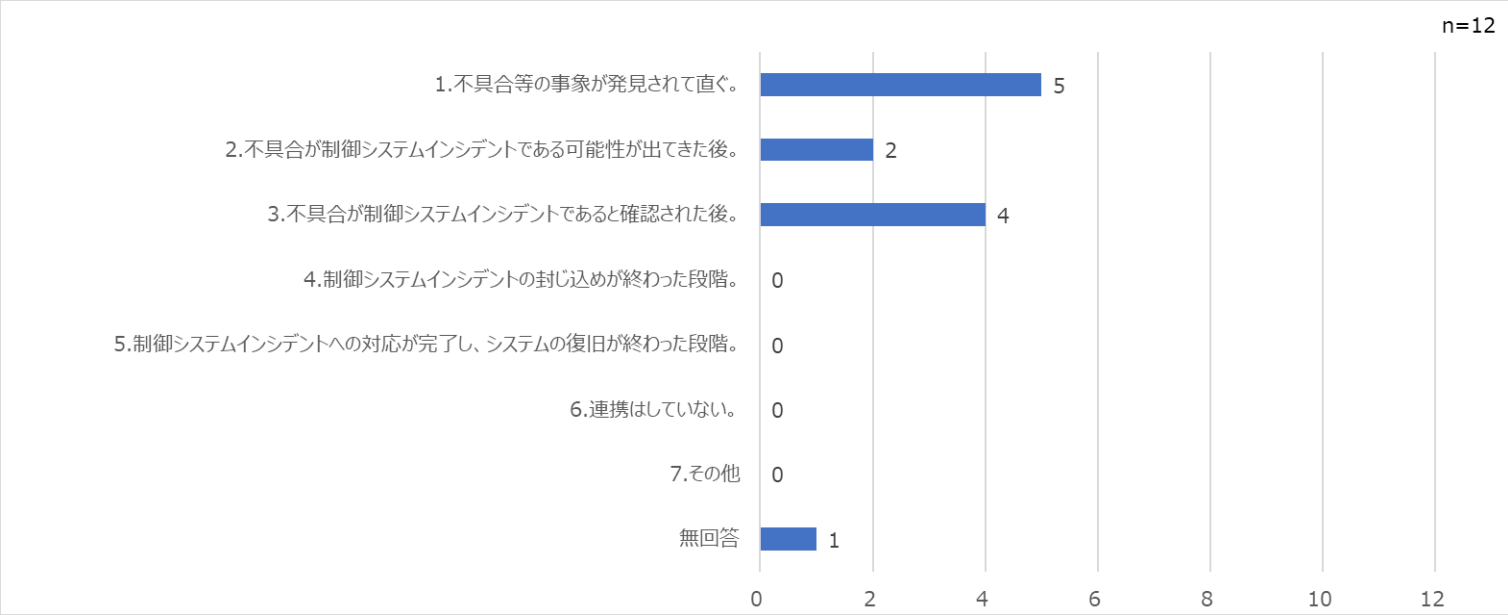
制御システムインシデントの影響範囲の確認方法（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• EDRの検知。 • 機械単体。 • 情報システムが発生の広がりを確認して、問題の制御システムから他への感染がない事を確認。 • 全PC系設備のマルウェアチェックを実施。

設問番号：5-3-10

経営層への報告・連携のタイミング

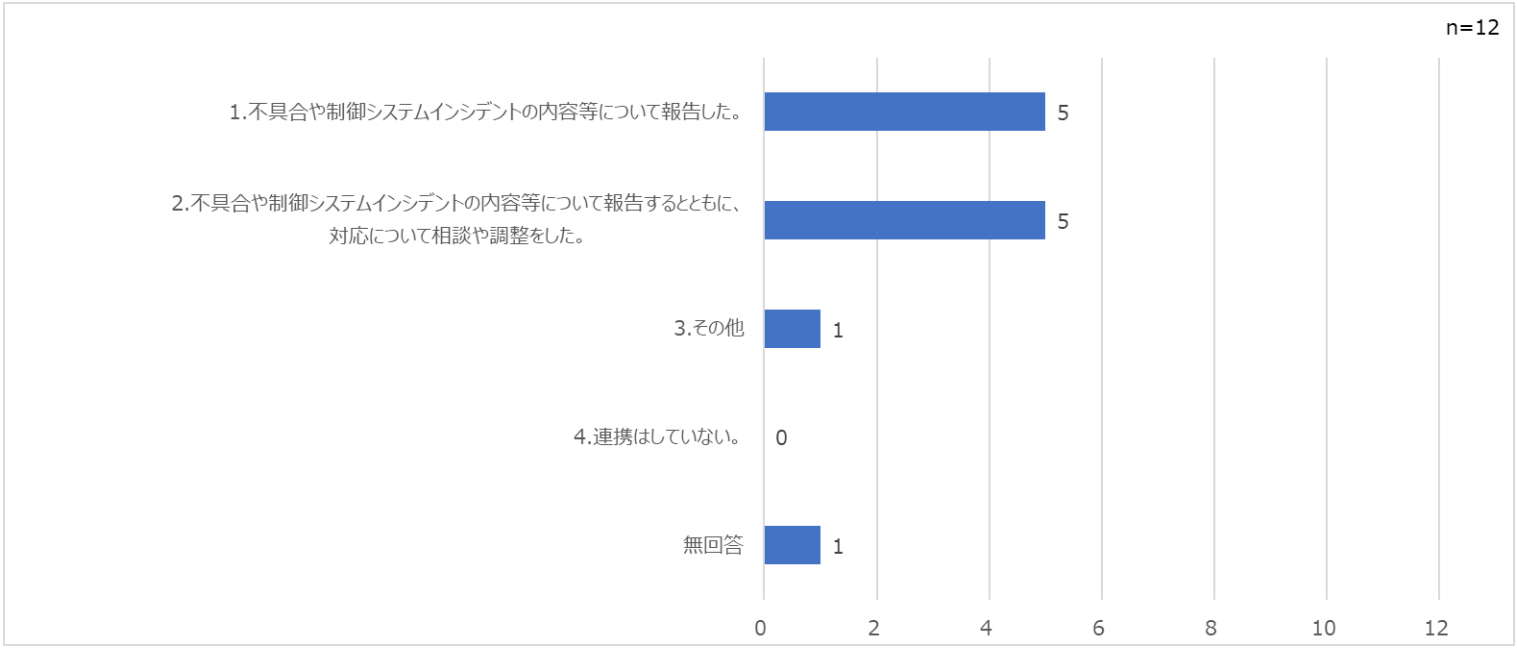
質問	その制御システムインシデントの発生に伴う、経営層への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-11

経営層への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、経営層への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-11

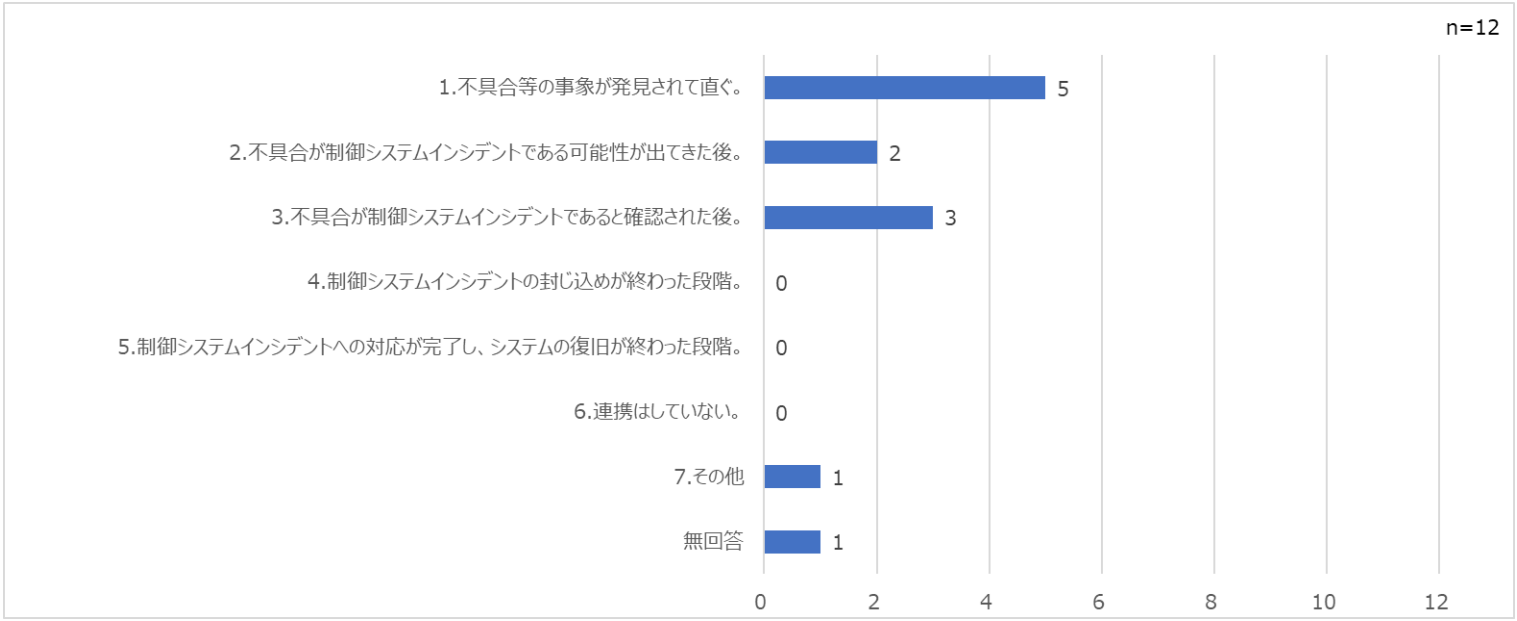
経営層への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 制御系システムか否かの判別前に、不正アクセス（ランサムウエア感染）報告を実施。その後、調査結果として制御系システムであることが判明した時点で報告。

設問番号：5-3-12

社内の関連SIRTや情報システム部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、社内の関連SIRTや情報システム部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-12

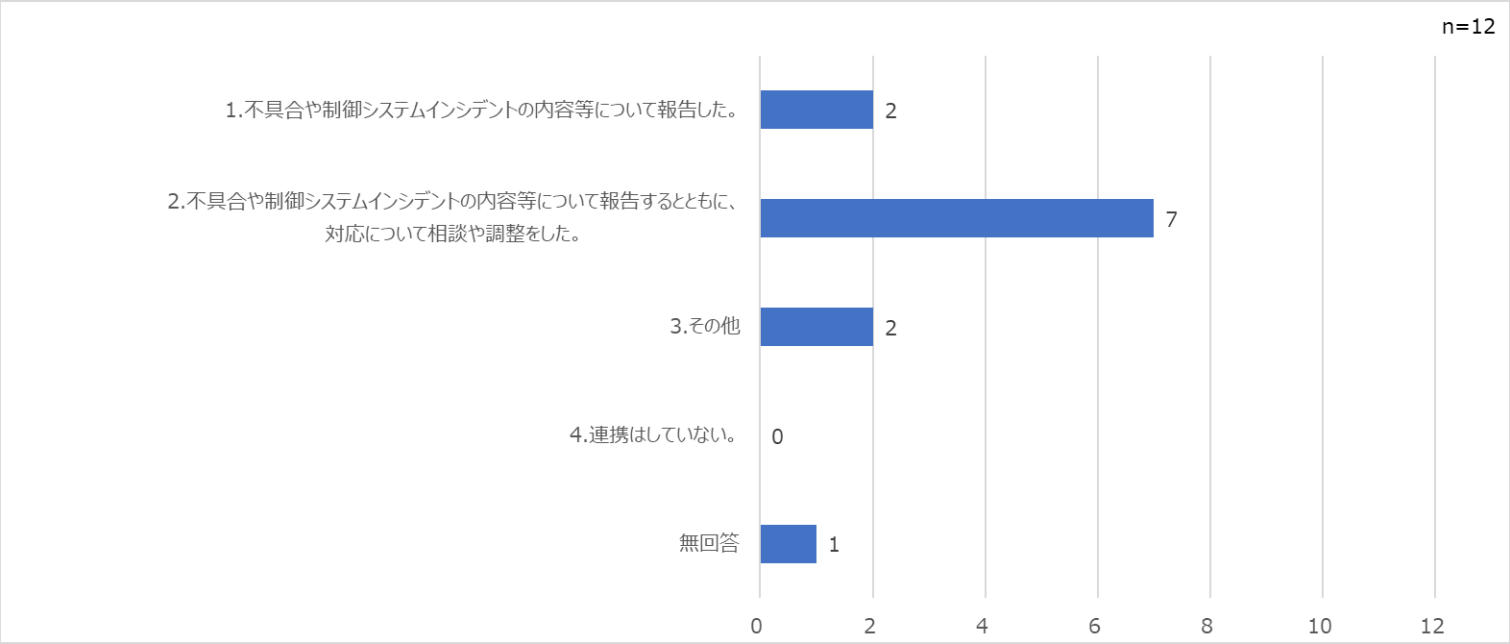
社内の関連SIRTや情報システム部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情シスで見つけた。

設問番号：5-3-13

社内の関連SIRTや情報システム部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、社内の関連SIRTや情報システム部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-13

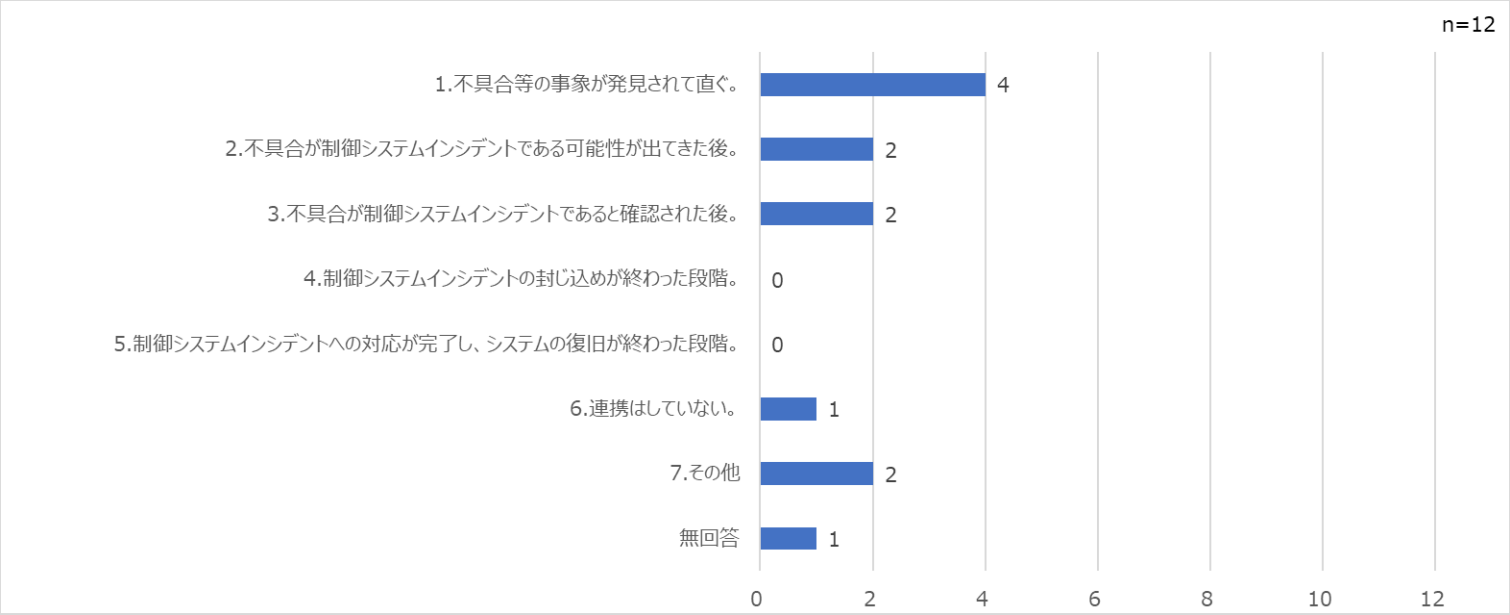
社内の関連SIRTや情報システム部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情シスで見つけた為、連携の必要なし。 • 制御系システムか否かの判別前に、不正アクセス（ランサムウエア感染）報告を実施。その後、調査結果として制御系システムであることが判明した時点で報告。

設問番号：5-3-14

製造システム部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、製造システム部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-14

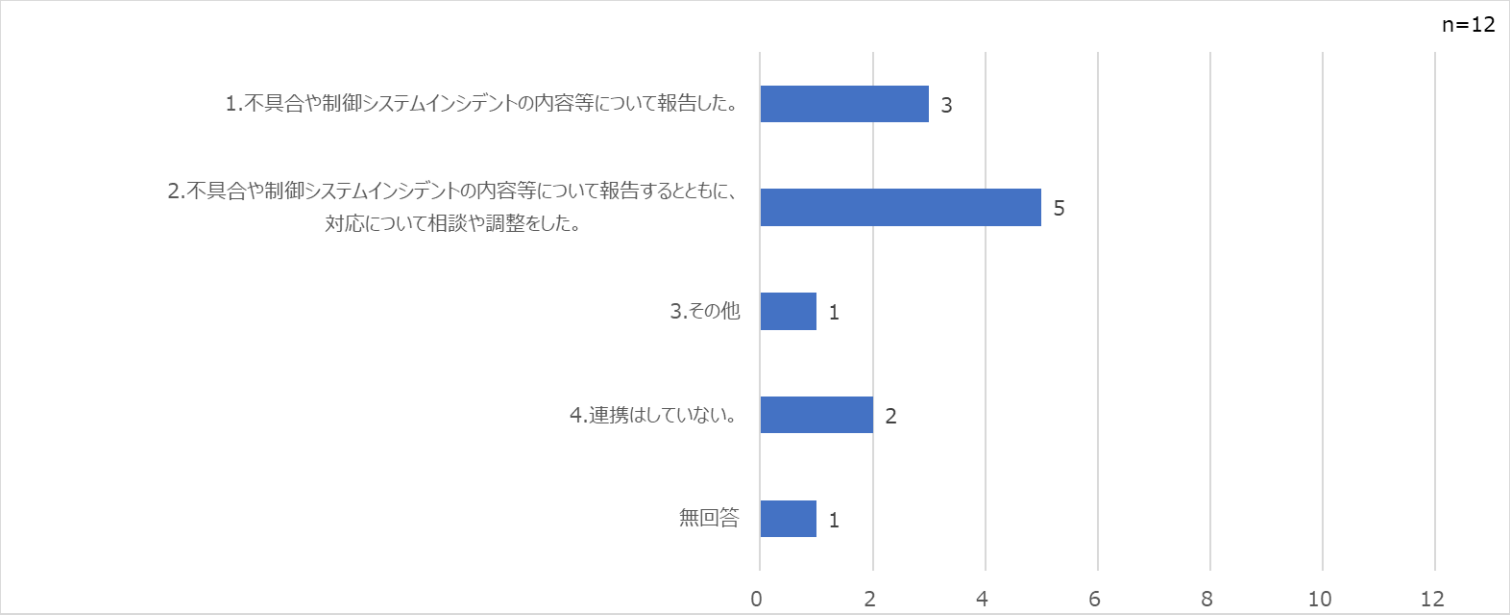
製造システム部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 最初の事象把握が製造システム部門である。 • 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • 製造部門は、拠点毎に存在する。よって、事象発見時に、不具合事象が発生した拠点のIT部門へ連絡し、拠点のIT部門から拠点内で連携している。

設問番号：5-3-15

製造システム部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、製造システム部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-15

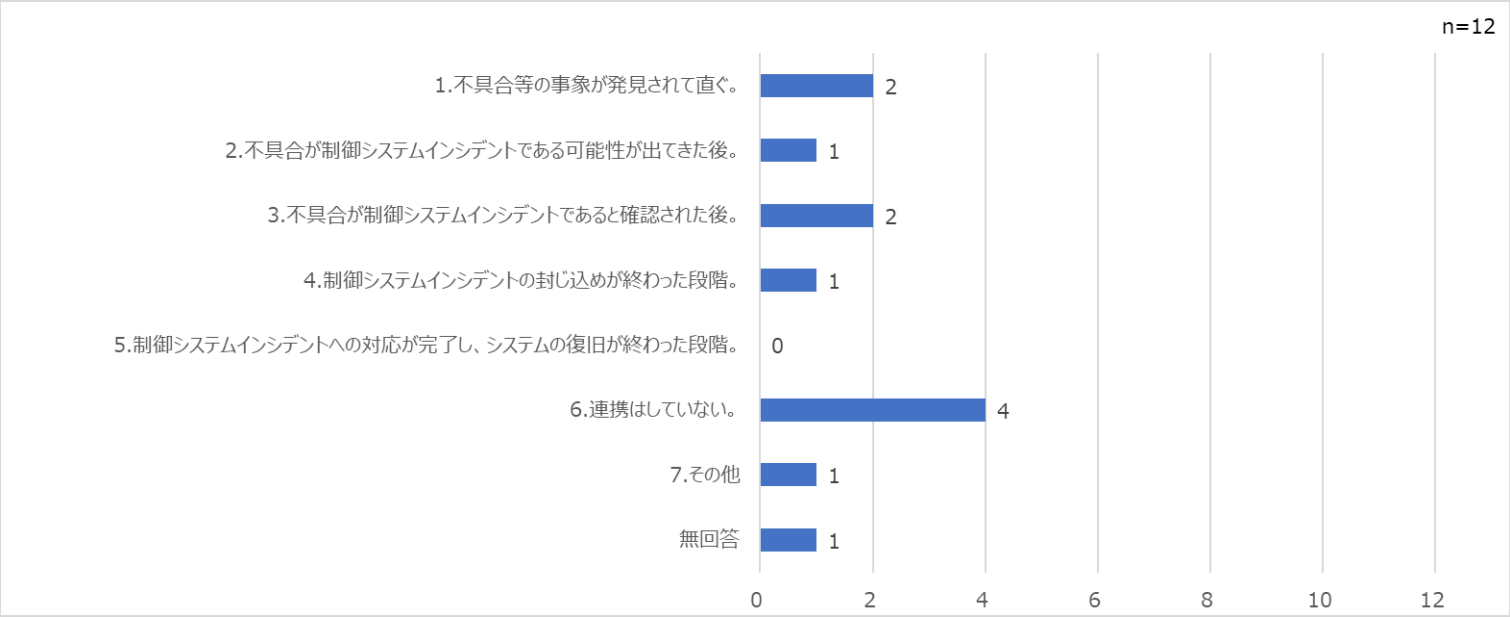
製造システム部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • 製造システム部門がサイバーセキュリティを統括する部門内の制御システムセキュリティ担当と連携・指導を受けて対応したため、報告も製造システム部門が主で行った。

設問番号：5-3-16

製品企画・開発部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、製品企画・開発部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-16

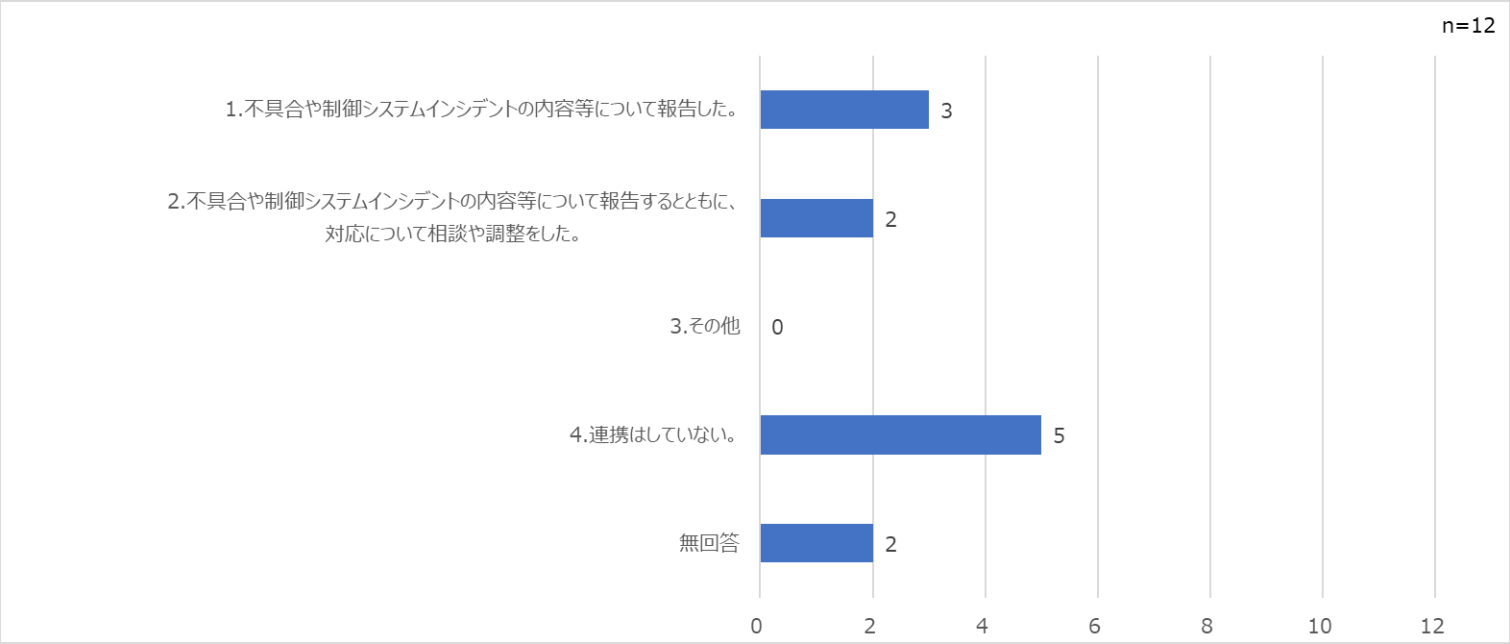
製品企画・開発部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • 製品企画・開発部門に影響のない事象であったため、個別に製品企画・開発部門に報告はしていない。

設問番号：5-3-17

製品企画・開発部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、製品企画・開発部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-17

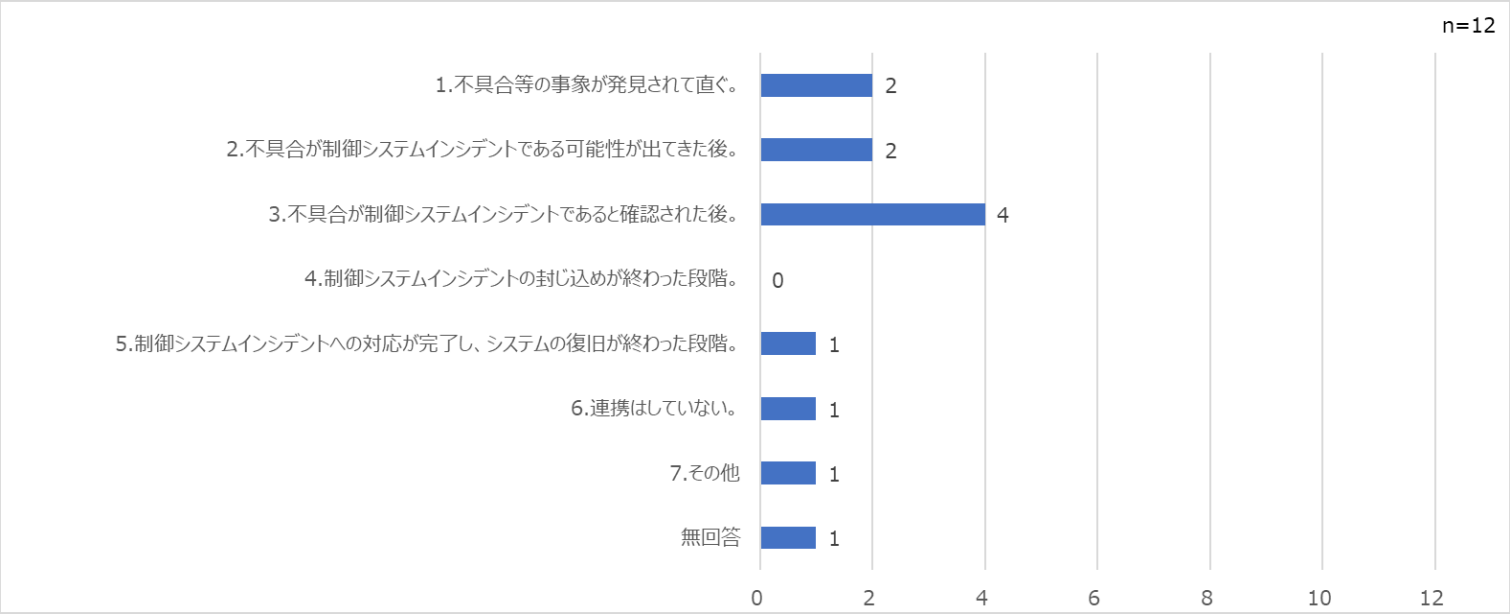
製品企画・開発部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。

設問番号：5-3-18

製造管理部門への報告・連携のタイミング

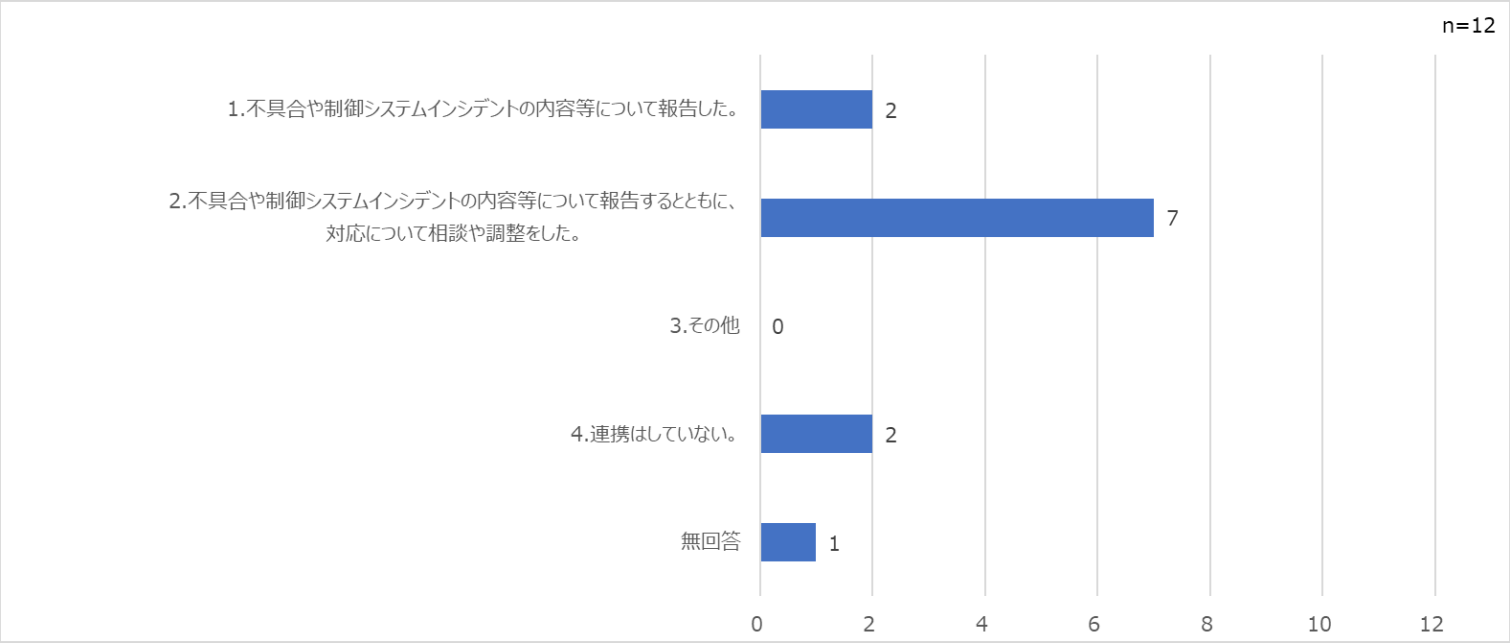
質問	その制御システムインシデントの発生に伴う、製造管理部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-19

製造管理部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、製造管理部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-19

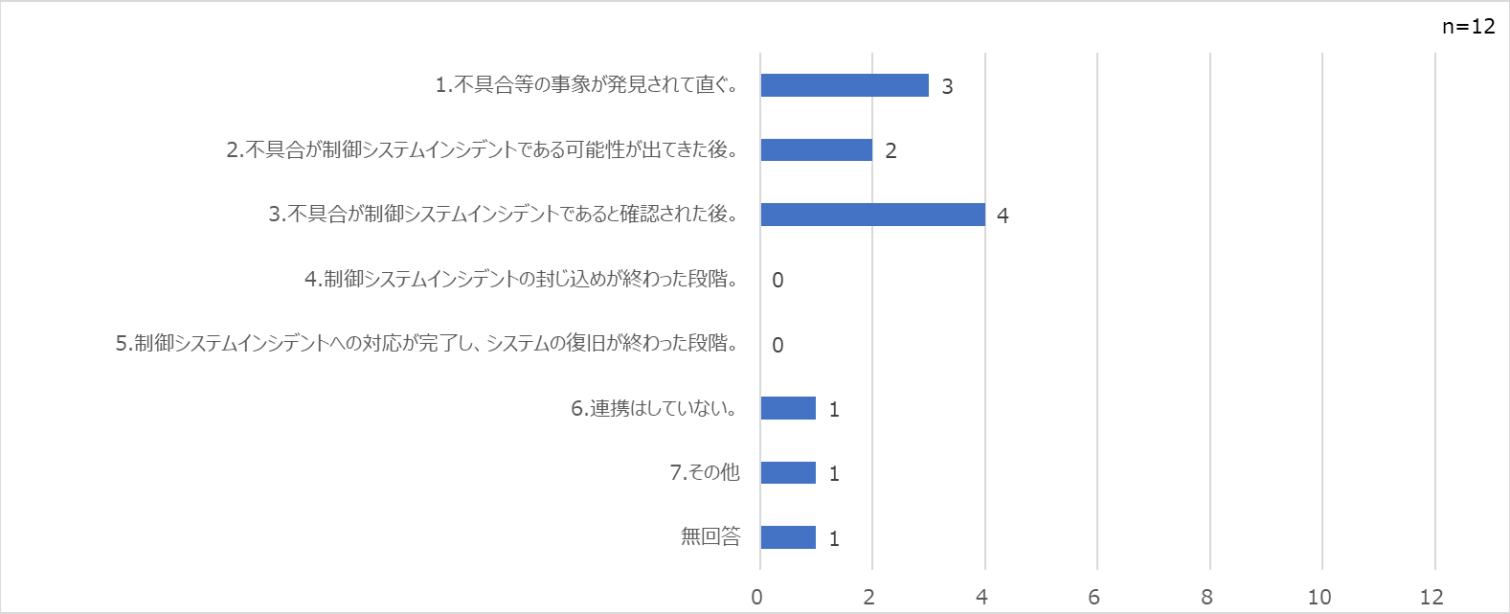
製造管理部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。

設問番号：5-3-20

製品製造部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、製品製造部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-20

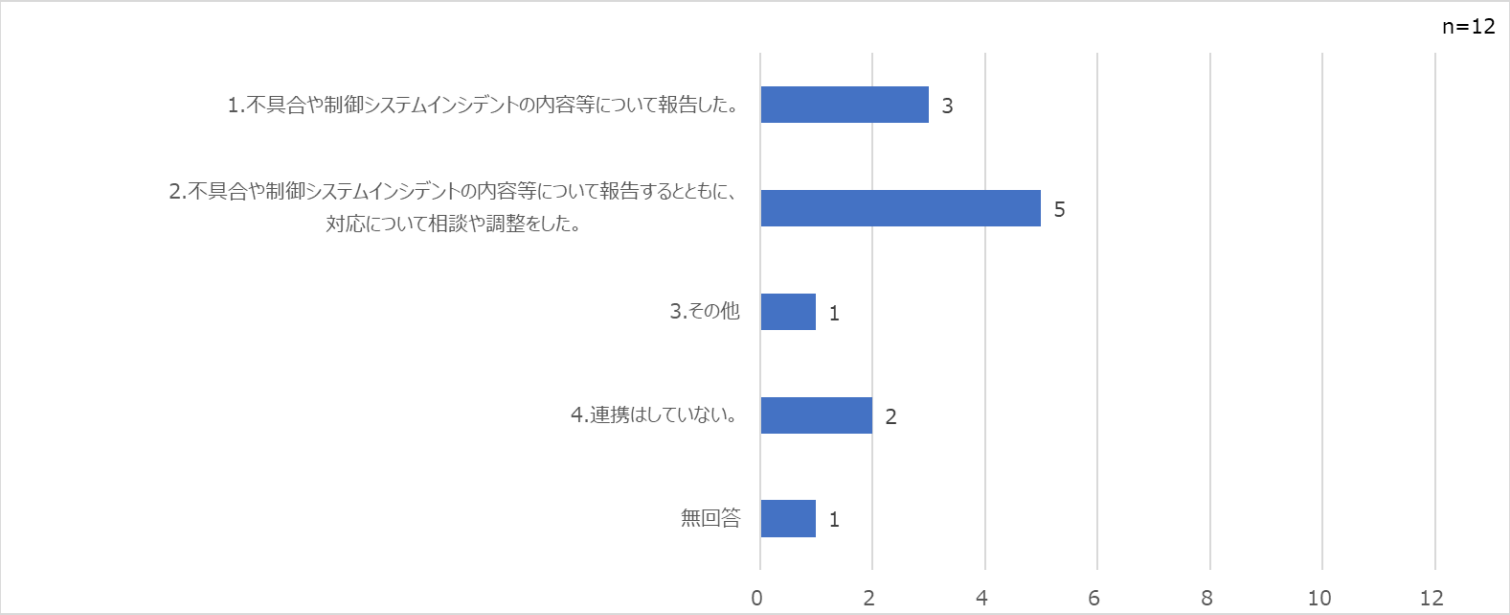
製品製造部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • その時点では拠点の製品製造部門へ直接報告する経路はない。拠点内の判断によるため、不明。

設問番号：5-3-21

製品製造部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、製品製造部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-21

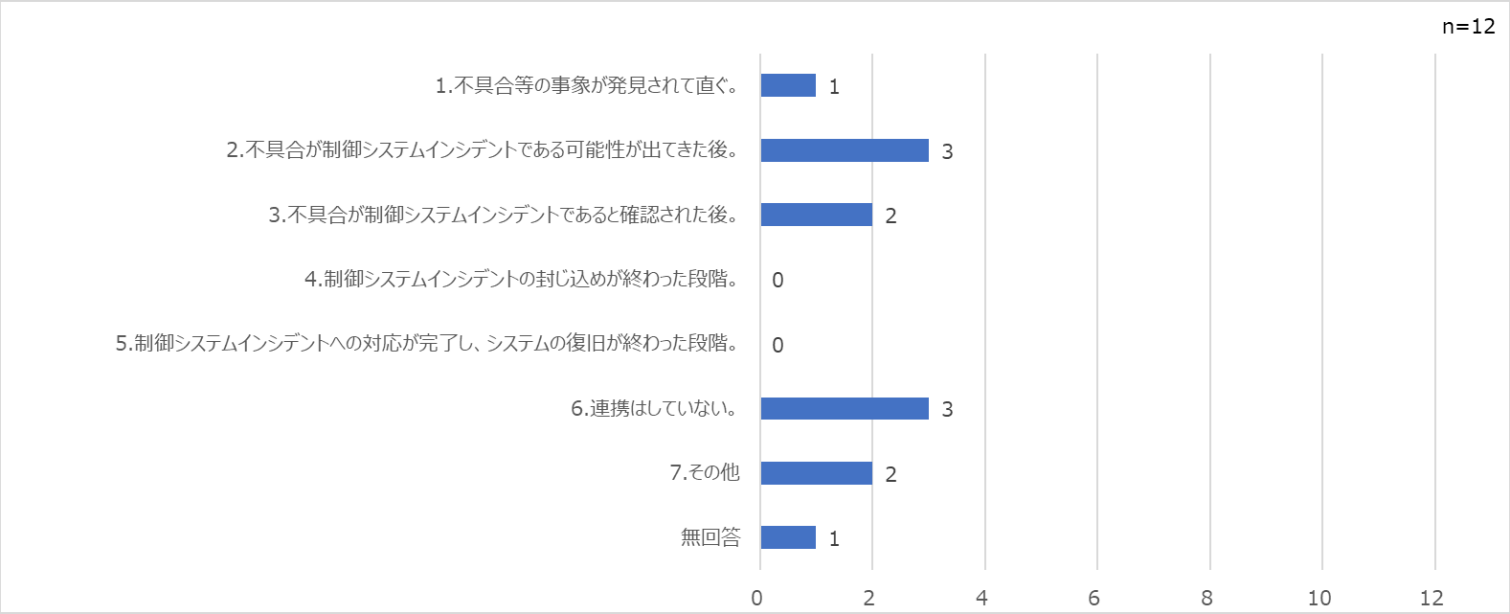
製品製造部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • 製品製造に直接影響が生じるインシデントではなかったため、インシデントの内容とともに一時的な監視機能の停止について対応と協力を依頼した。

設問番号：5-3-22

品質管理部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、品質管理部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-22

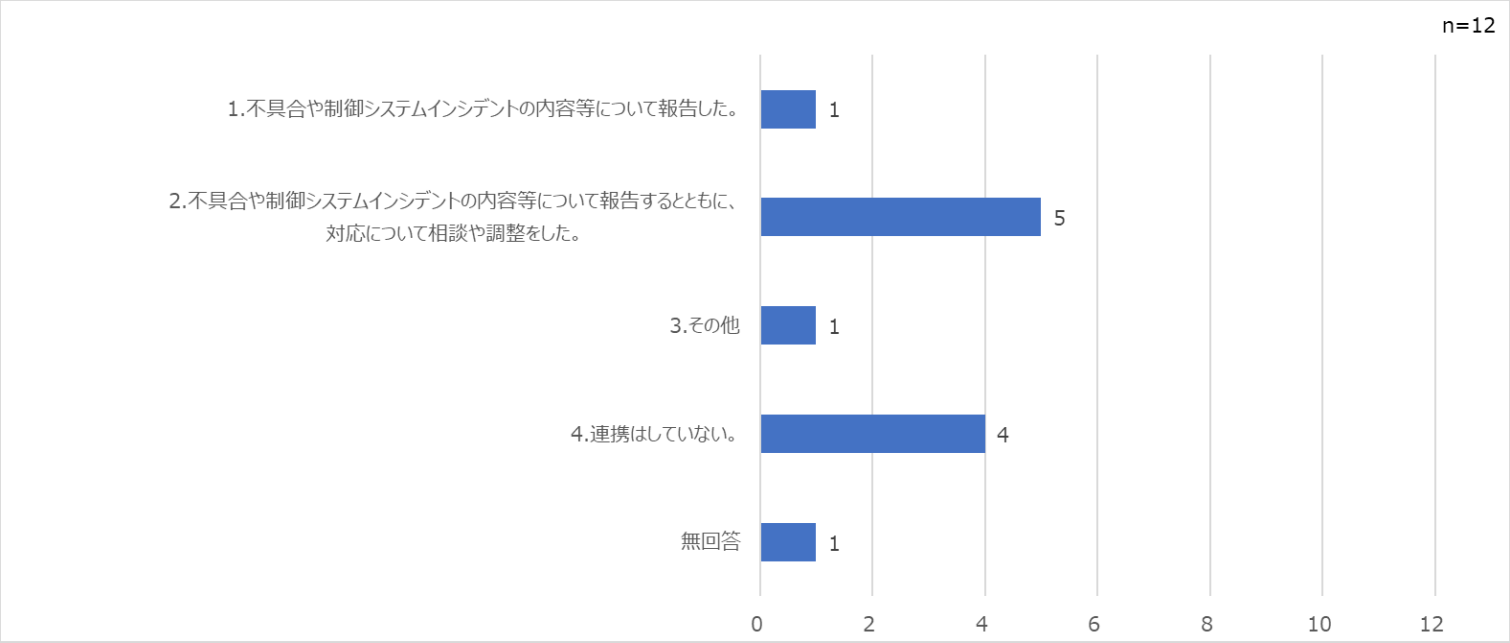
品質管理部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • その時点では拠点の品質管理部門へ報告する直接経路はない。拠点内の判断によるため、不明。 • 品質管理部門に影響のない事象であったため、個別に品質管理部門に報告はしていない。

設問番号：5-3-23

品質管理部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、品質管理部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-23

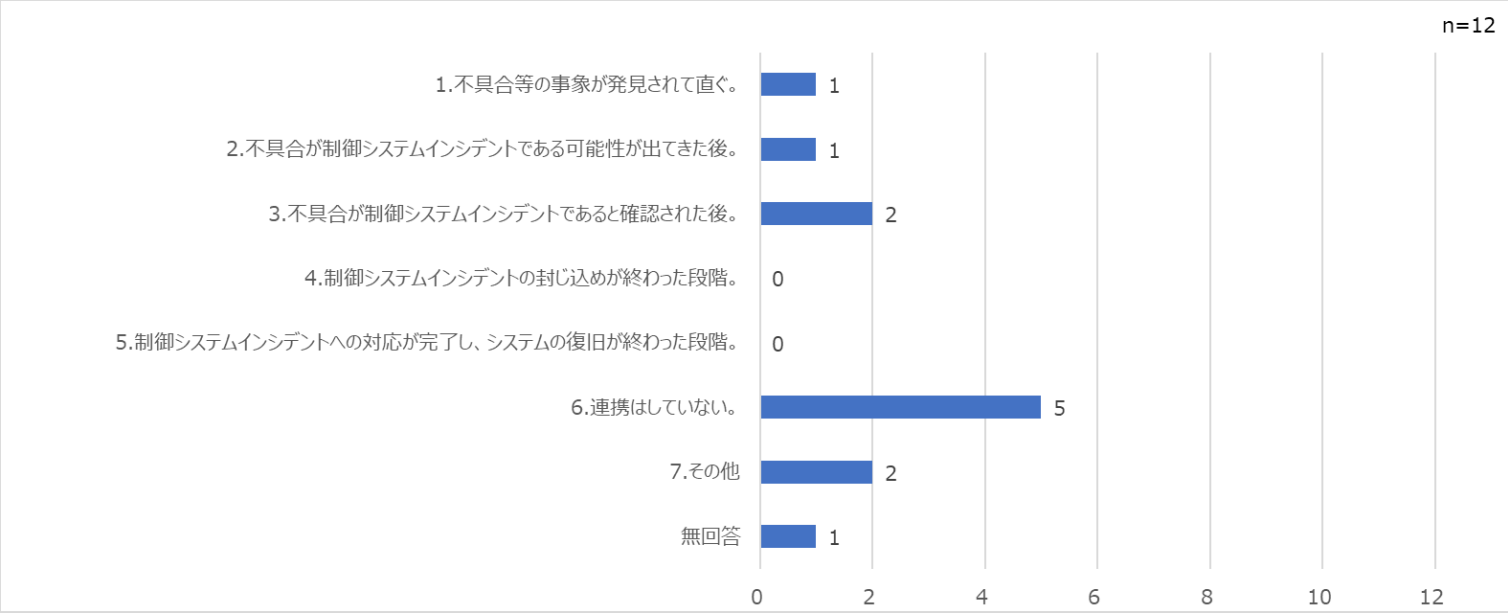
品質管理部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • その時点では拠点の品質管理部門へ報告する直接経路はない。拠点内の判断によるため、不明。

設問番号：5-3-24

保安部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、保安部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-24

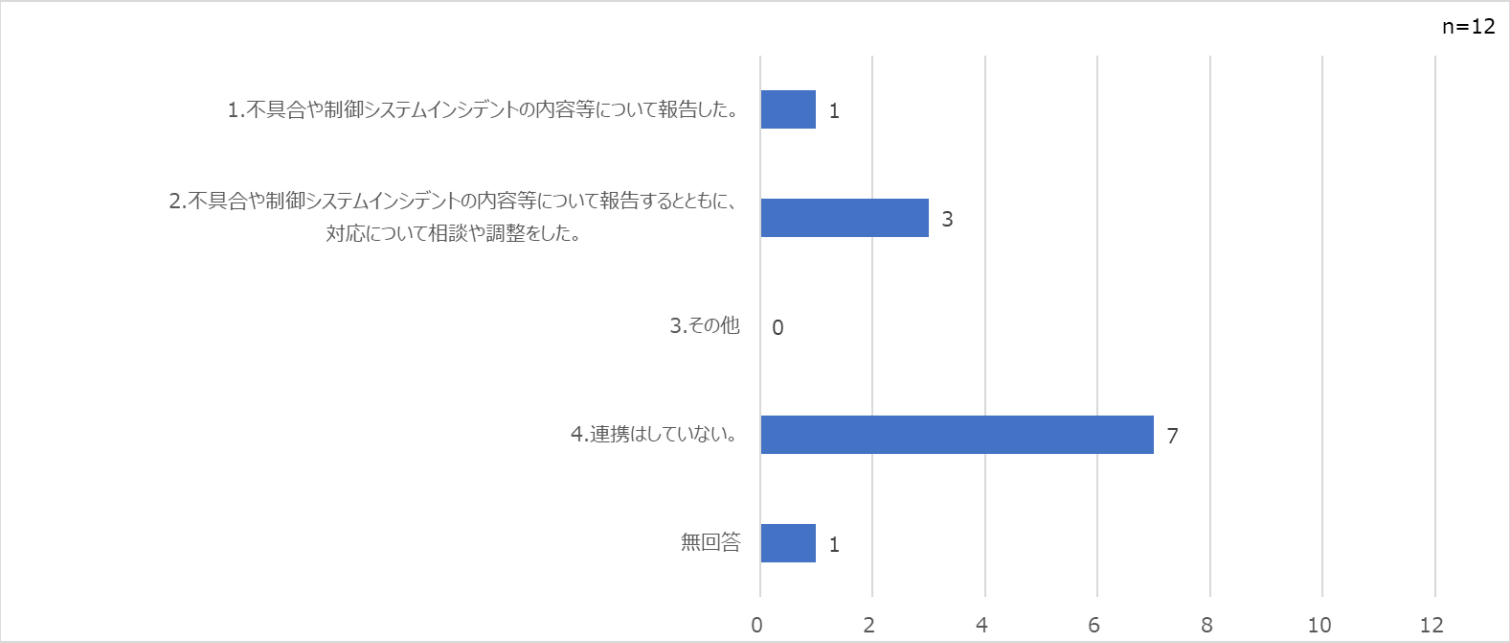
保安部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • その時点では拠点の保安部門へ報告する直接経路はない。拠点内の判断によるため、不明。 • 保安部門はない。

設問番号：5-3-25

保安部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、保安部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-25

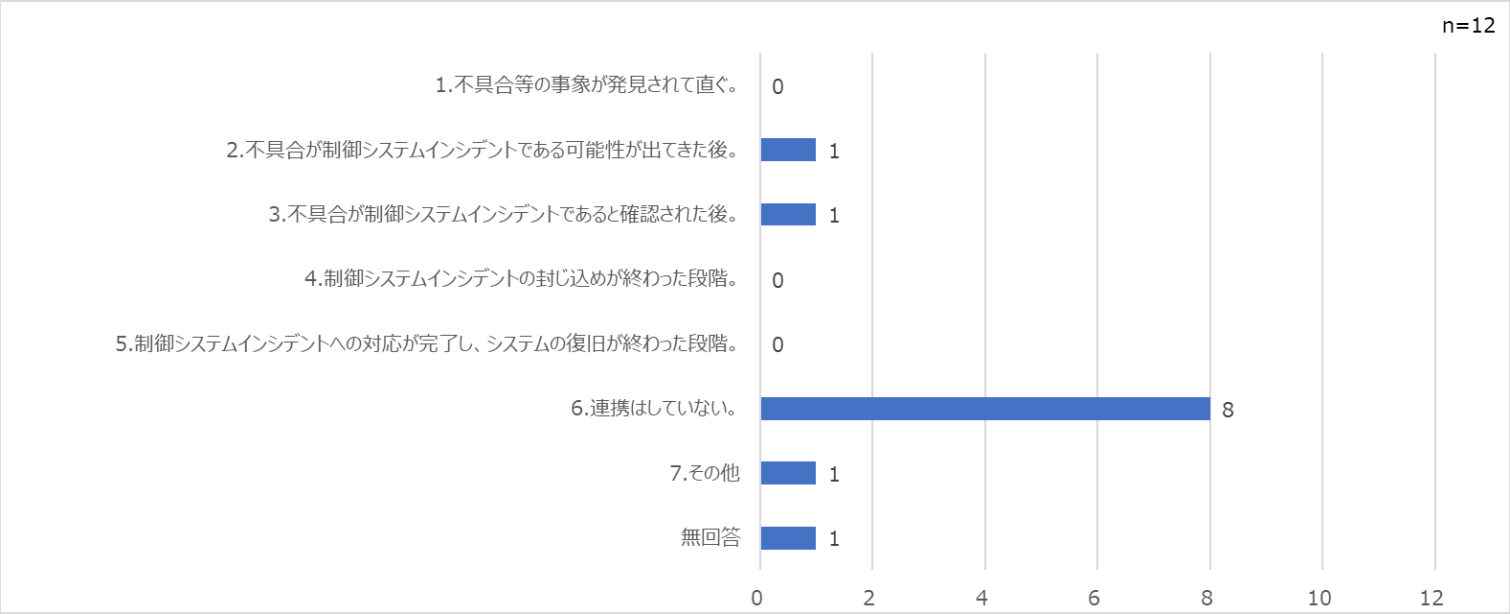
保安部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • 保安部門はない。

設問番号：5-3-26

法務部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、法務部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-26

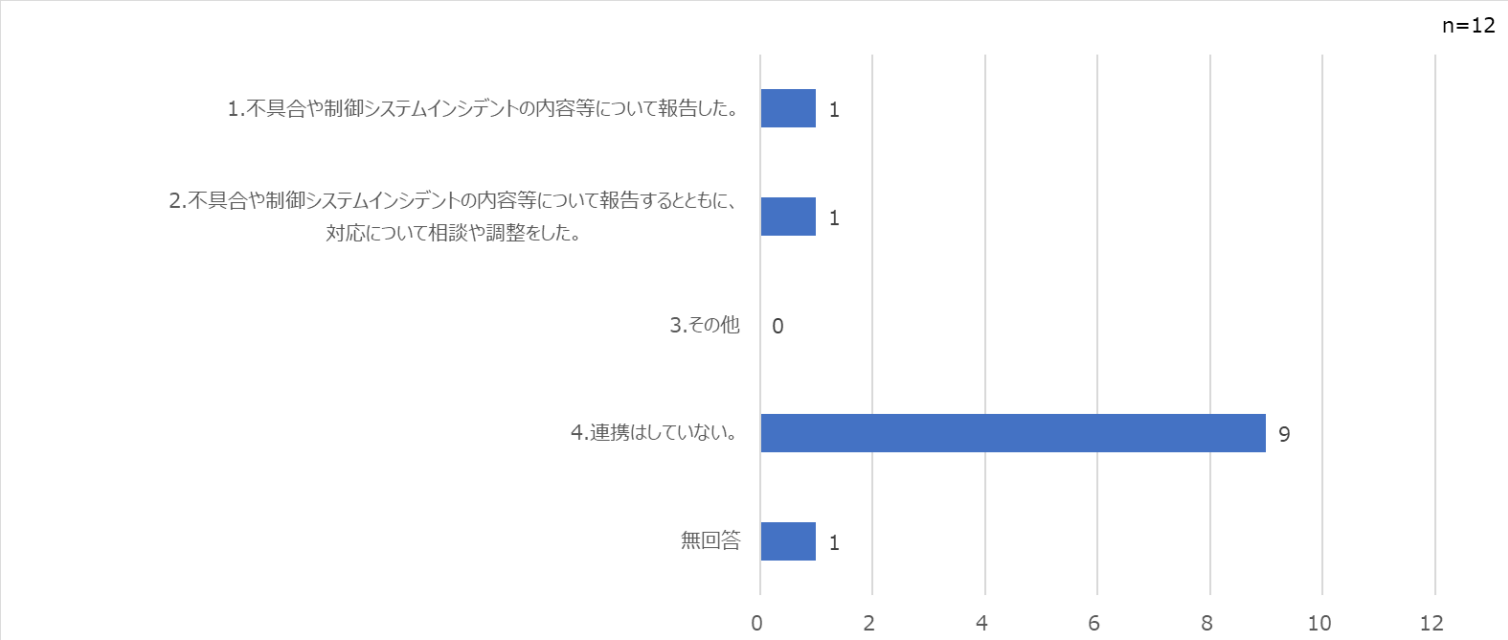
法務部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • 拠点が関係会社であるため、当該拠点の判断による。

設問番号：5-3-27

法務部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、法務部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-27

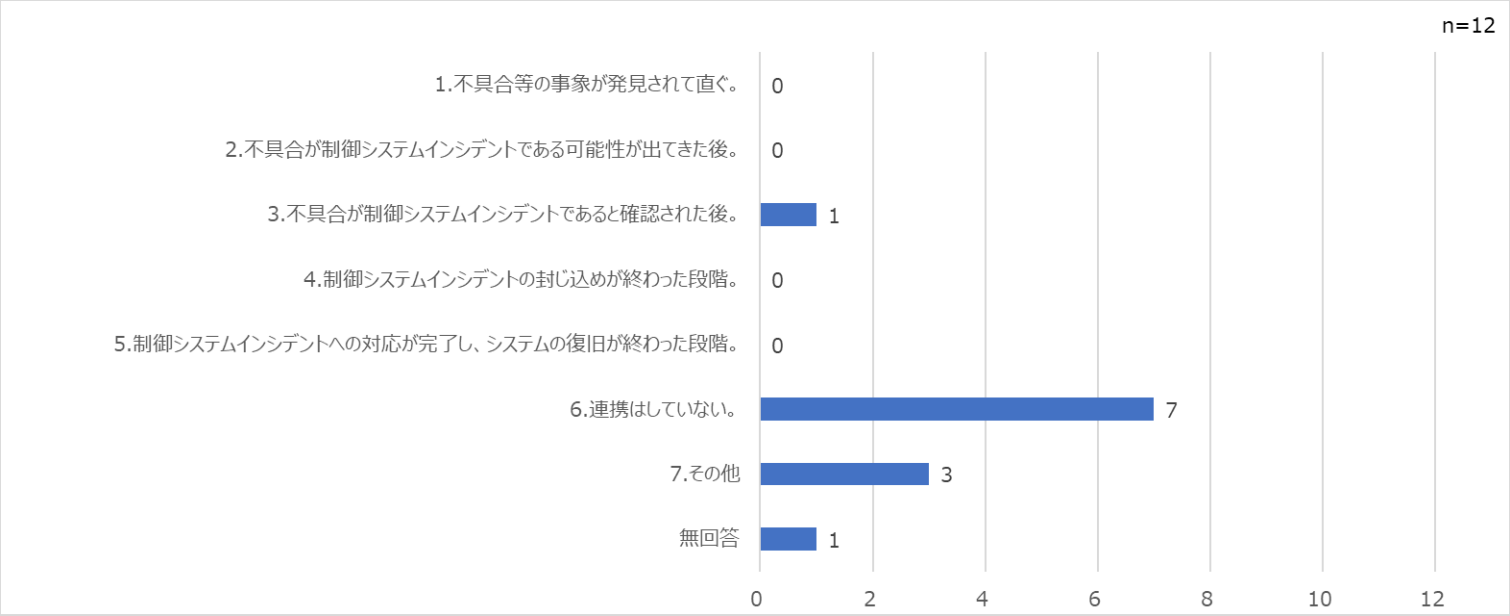
法務部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。

設問番号：5-3-28

広報部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、広報部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-28

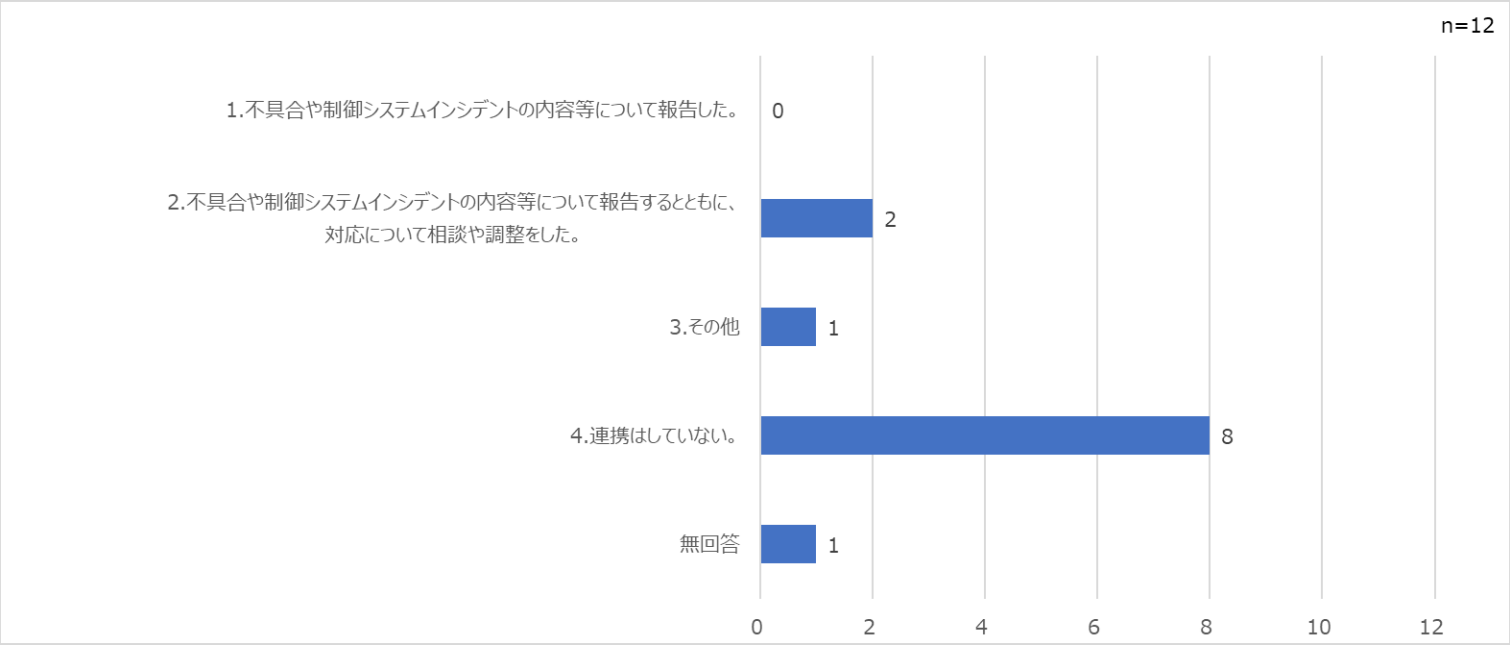
広報部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • 拠点が関係会社であるため、当該拠点の判断による。 • 広報部門はない。

設問番号：5-3-29

広報部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、広報部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-29

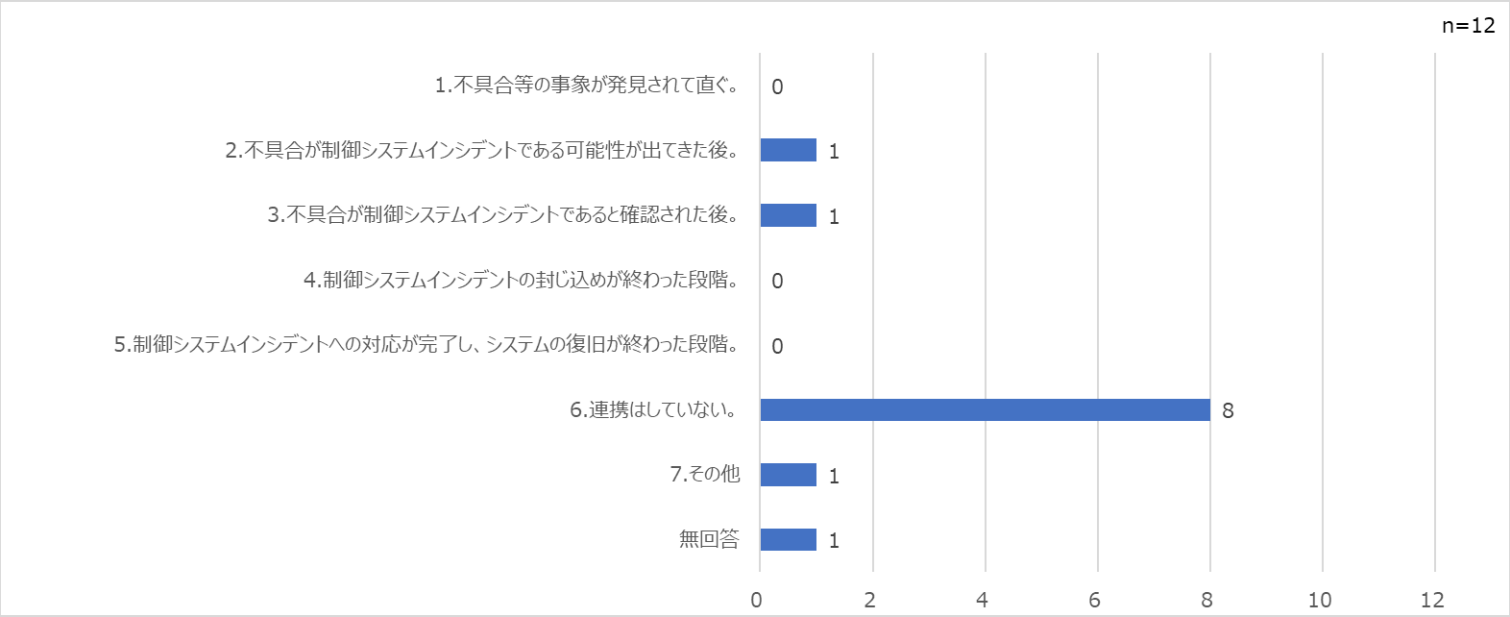
広報部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。 • 広報部門はない。

設問番号：5-3-30

営業部門への報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、営業部門への報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-30

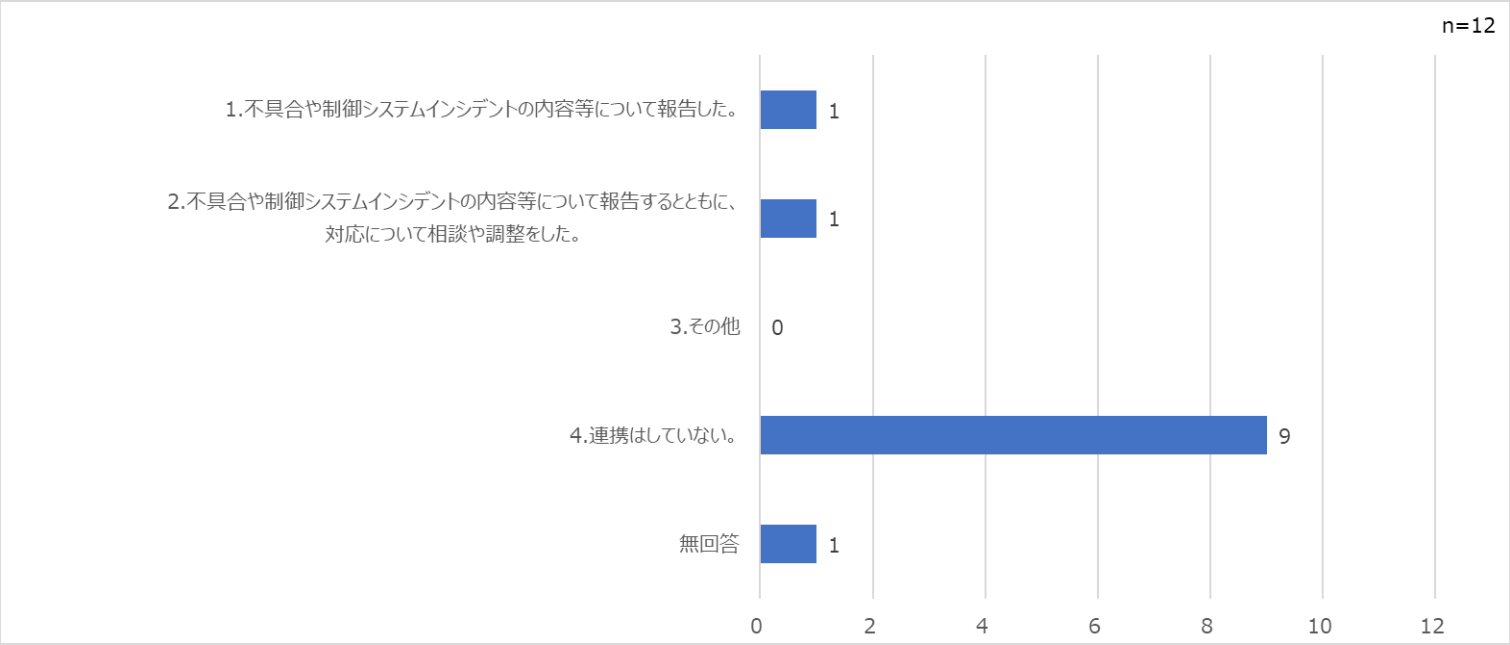
営業部門への報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 事業部門毎の判断による。 • 情報システムから他への感染がない事の報告を受けて、連携は行っていない。

設問番号：5-3-31

営業部門への報告・連携の内容（1/2）

質問	その制御システムインシデントの発生に伴う、営業部門への報告・連携の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-31

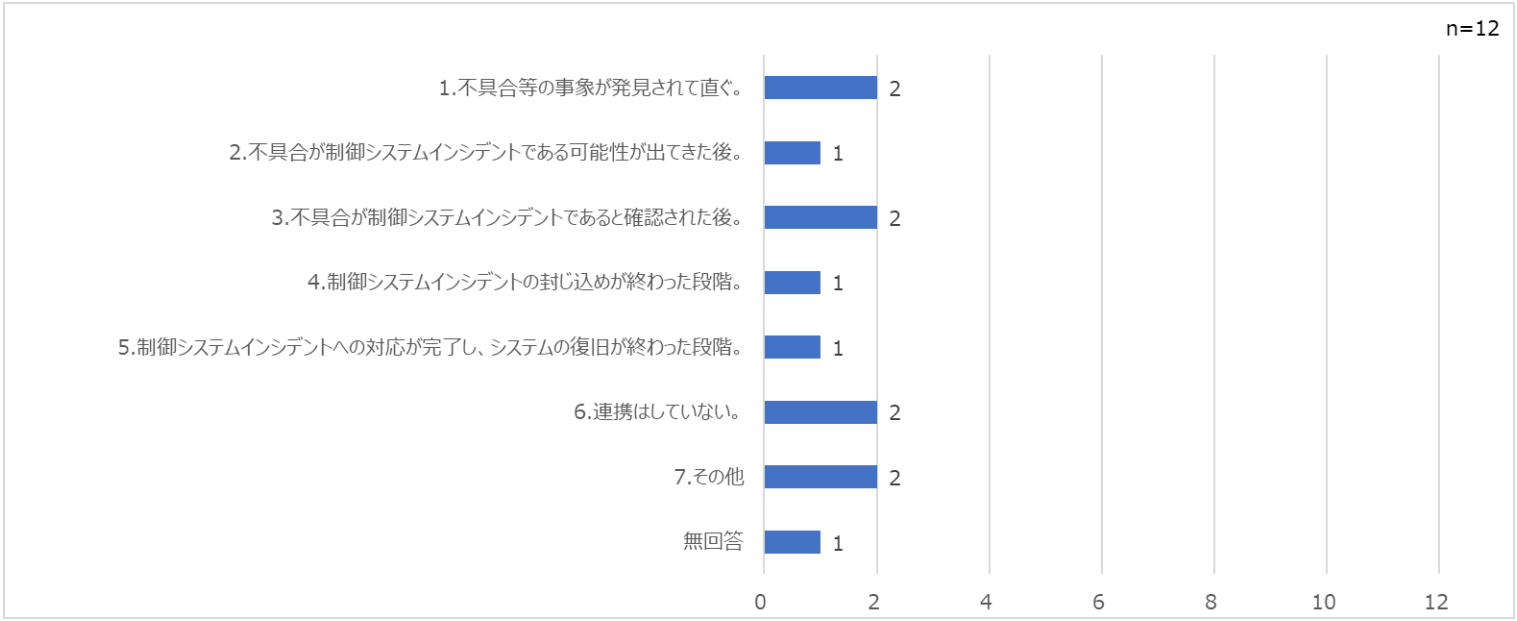
営業部門への報告・連携の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 情報システムから他への感染がない事の報告を受けて、連携は行っていない。

設問番号：5-3-32

制御システムに係るシステムベンダや機器ベンダへの報告・連携のタイミング（1/2）

質問	その制御システムインシデントの発生に伴う、制御システムに係るシステムベンダや機器ベンダへの報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-32

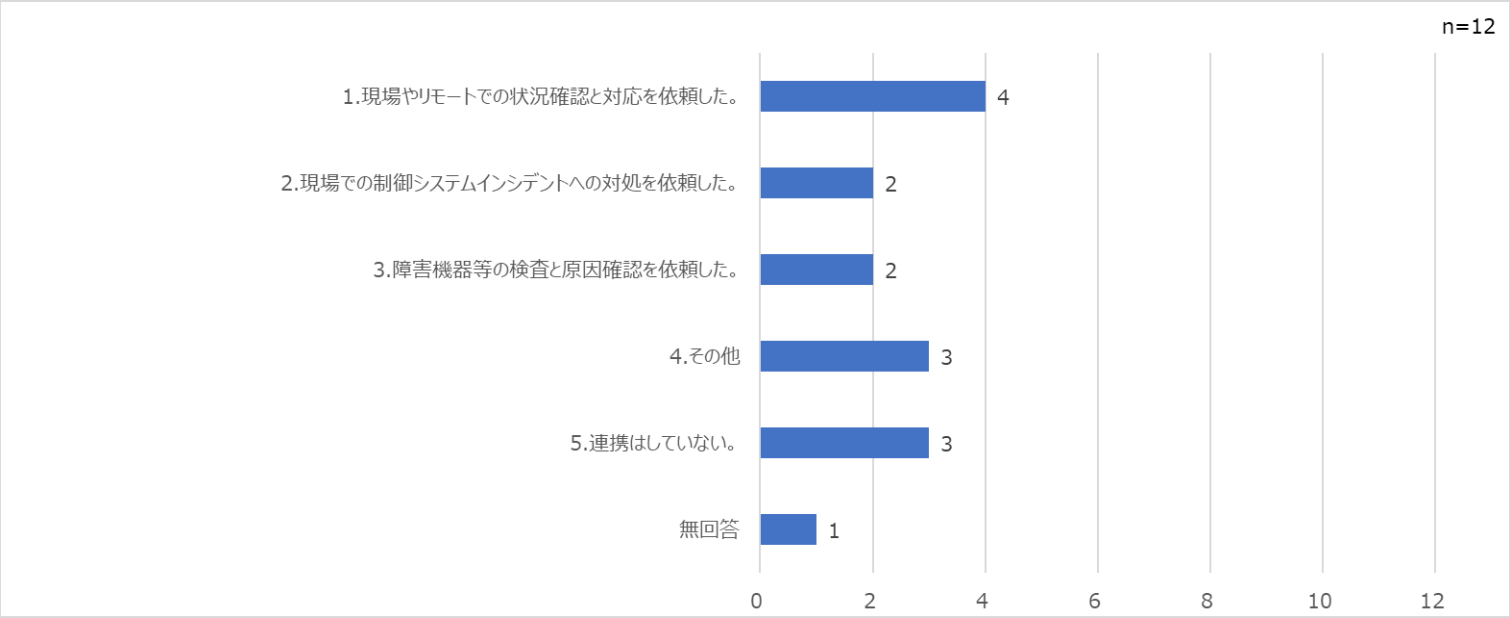
制御システムに係るシステムベンダや機器ベンダへの報告・連携のタイミング（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• ベンダ機器の不具合によるものではないことが判明している。 • 連携すべきベンダなし。

設問番号：5-3-33

制御システムに係るシステムベンダや機器ベンダへの支援依頼等の内容（1/2）

質問	その制御システムインシデントの発生に伴う、制御システムに係るシステムベンダや機器ベンダへの支援依頼等の内容についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-3-33

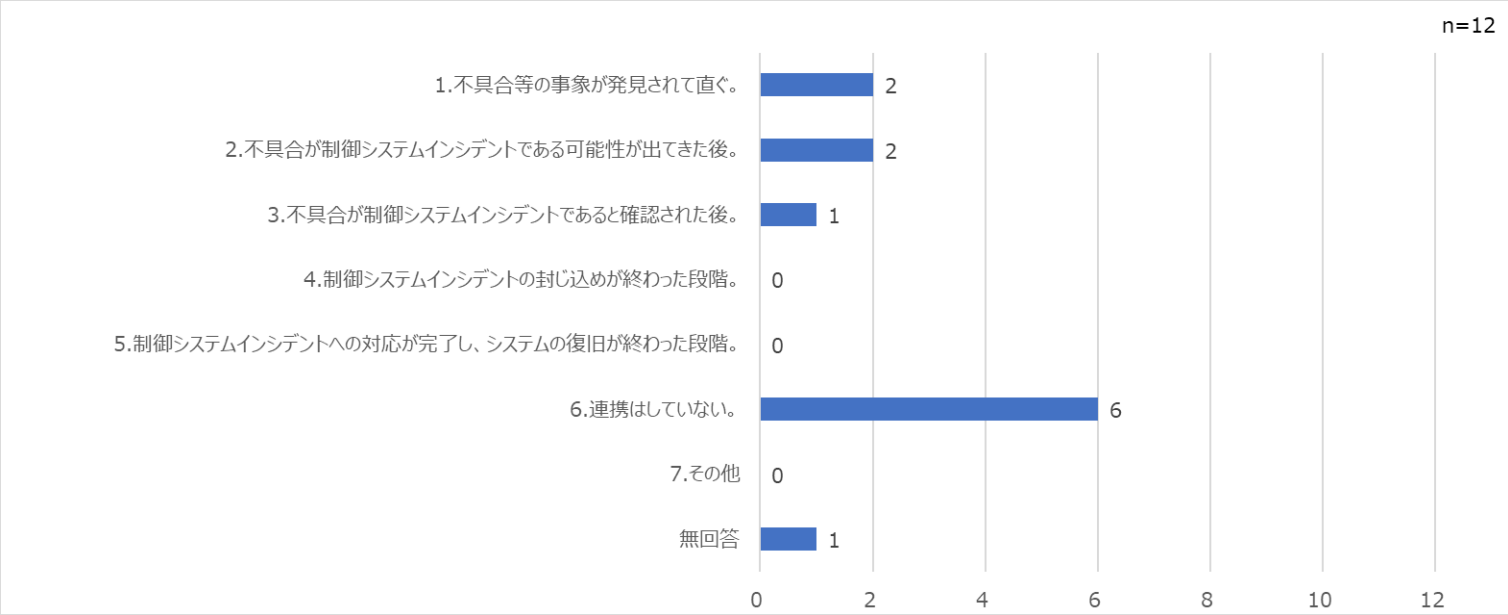
制御システムに係るシステムベンダや機器ベンダへの支援依頼等の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 現状システムの仕様確認と対策についての相談は実施したが、インシデント対応自体の支援は依頼していない。 • マルウェア感染の事実を伝えた。 • 連携すべきベンダはなし。

設問番号：5-3-34

セキュリティベンダへの報告・連携のタイミング

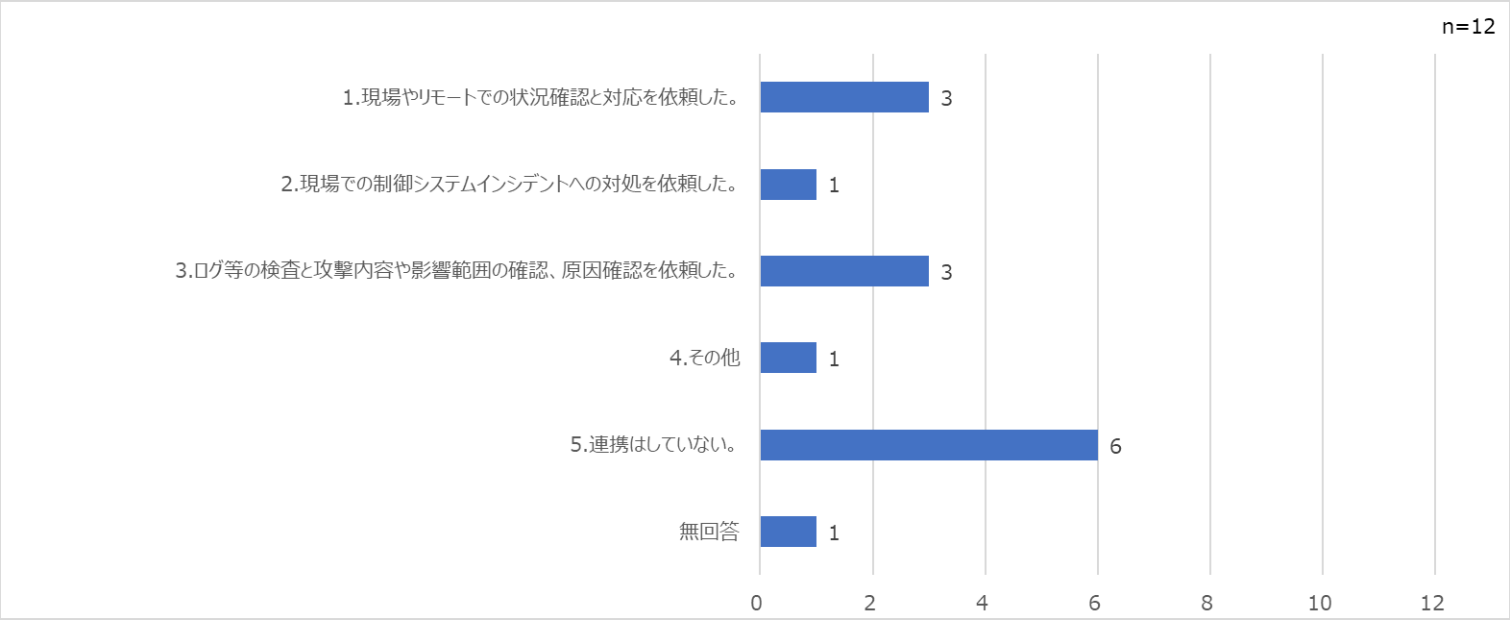
質問	その制御システムインシデントの発生に伴う、セキュリティベンダへの報告・連携のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-35

セキュリティベンダへの支援依頼の内容（1/2）

質問	その制御システムインシデントの発生に伴う、セキュリティベンダへの支援依頼の内容についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-3-35

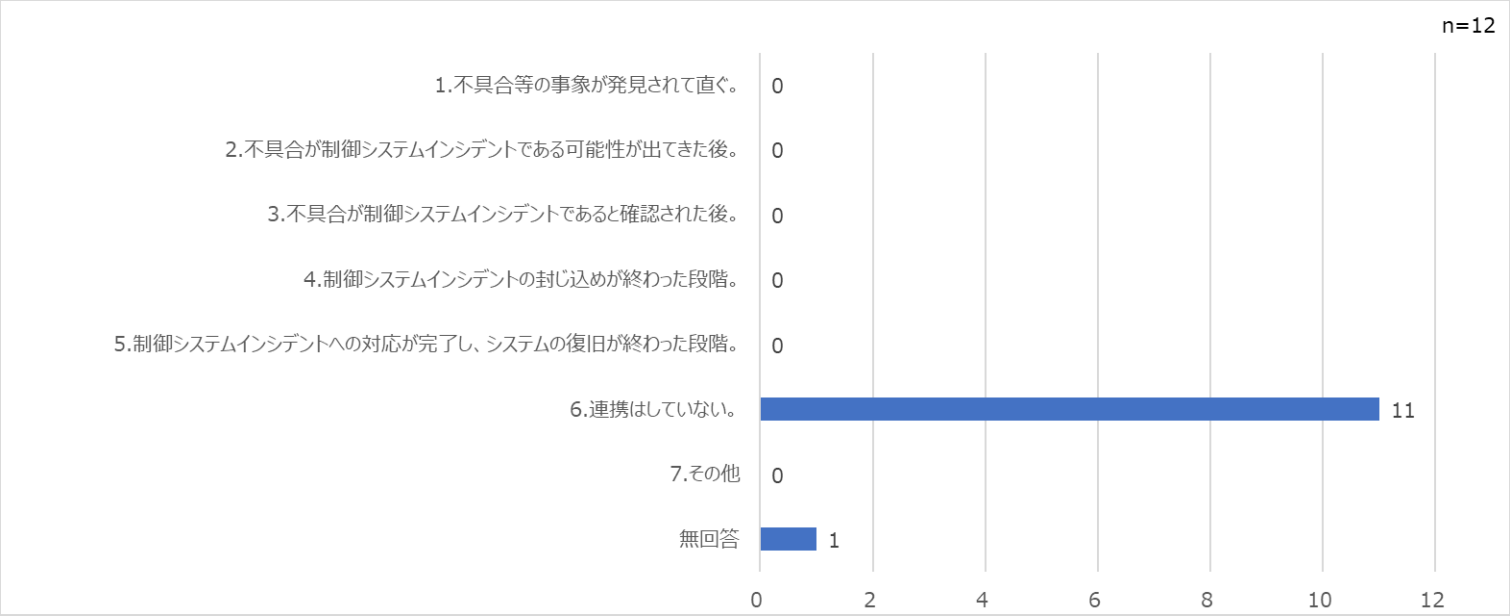
セキュリティベンダへの支援依頼の内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• EDR機能での自動隔離。

設問番号：5-3-36

JPCERT/CCへの報告・連携のタイミング

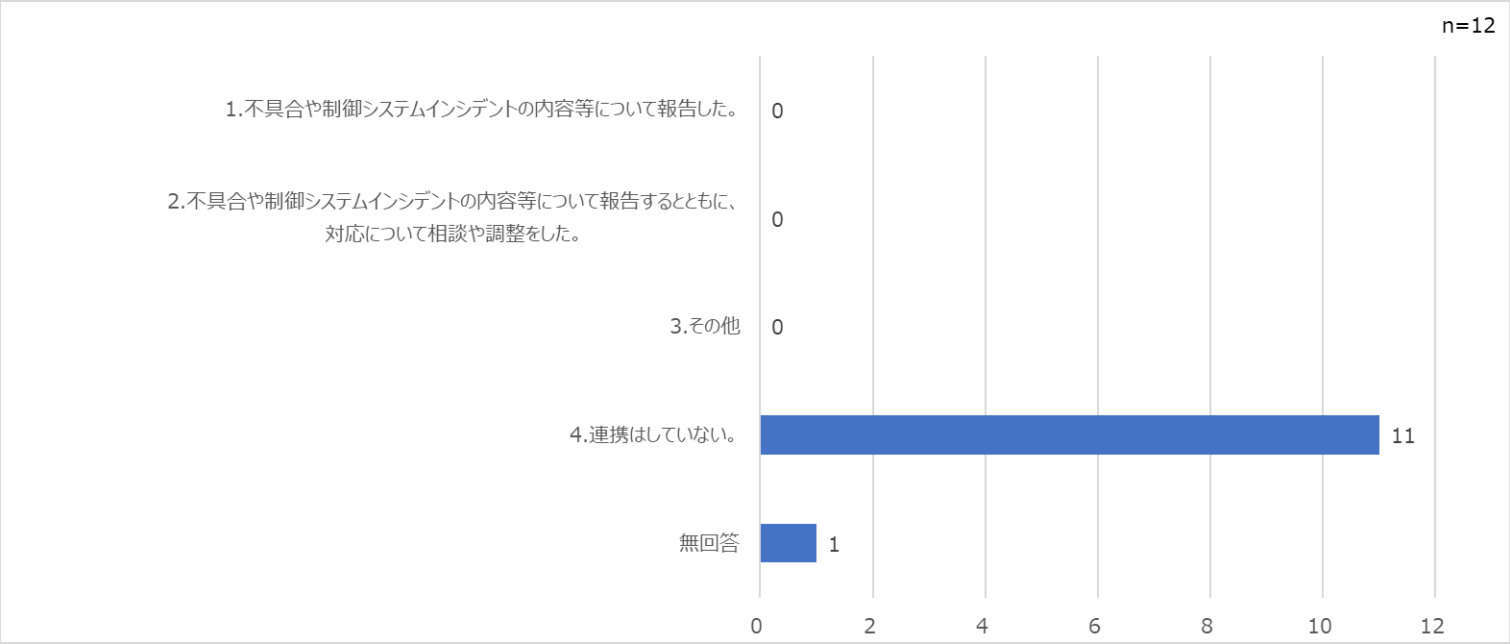
質問	その制御システムインシデントの発生に伴う、公的な窓口（JPCERT/CC）への報告・連携（対応相談）のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-37

JPCERT/CCへの報告・連携の内容

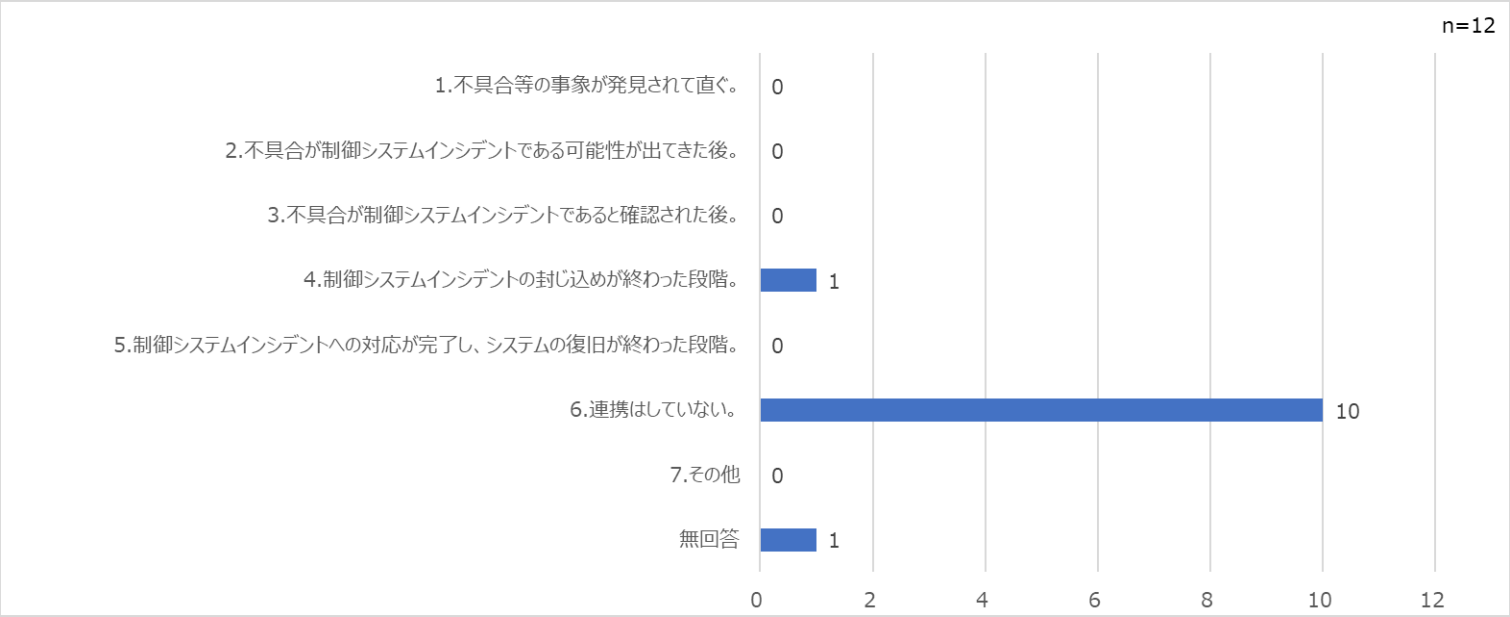
質問	その制御システムインシデントの発生に伴う、公的な窓口（JPCERT/CC）への報告・連携（対応相談）の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-38

サイバーセキュリティ情報の共有団体への報告・連携のタイミング

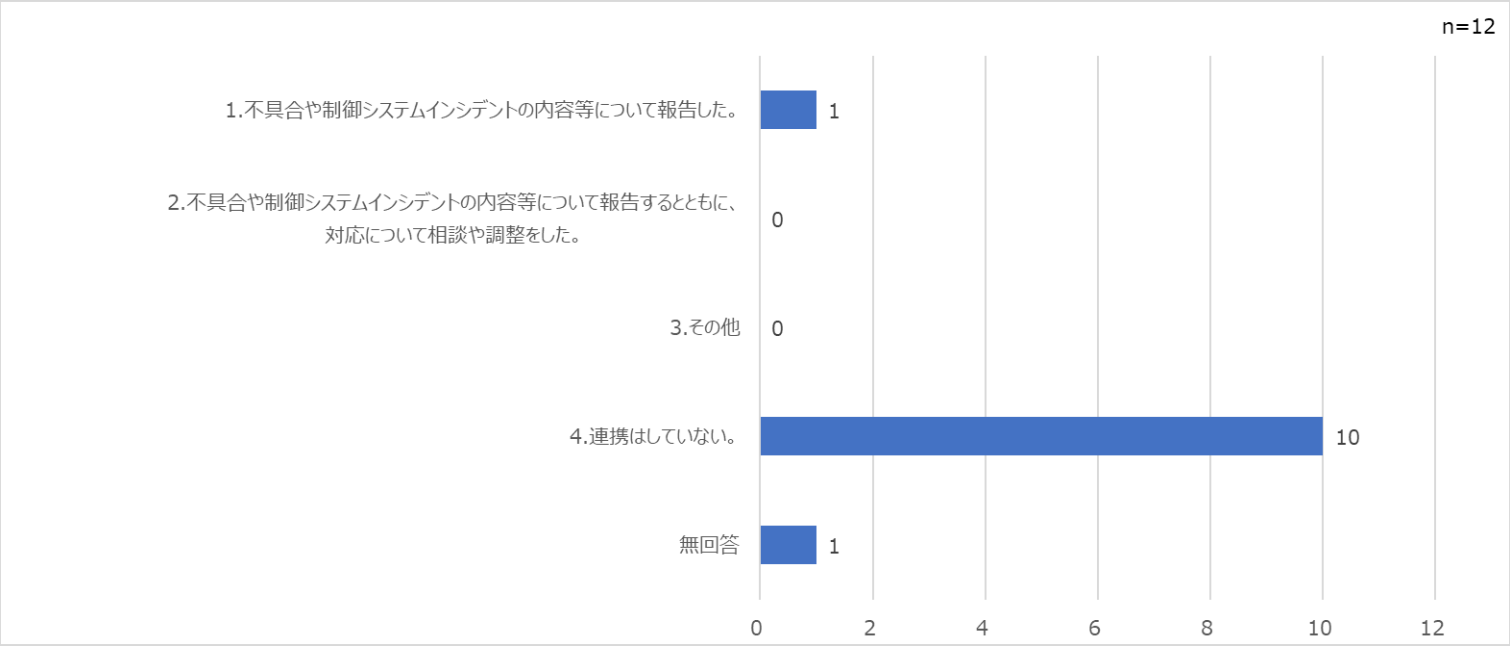
質問	その制御システムインシデントの発生に伴う、公的な窓口（所属するサイバーセキュリティ情報の共有団体（ISAC、セプター、業界団体等））への報告・連携（対応相談）のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-39

サイバーセキュリティ情報の共有団体への報告・連携の内容

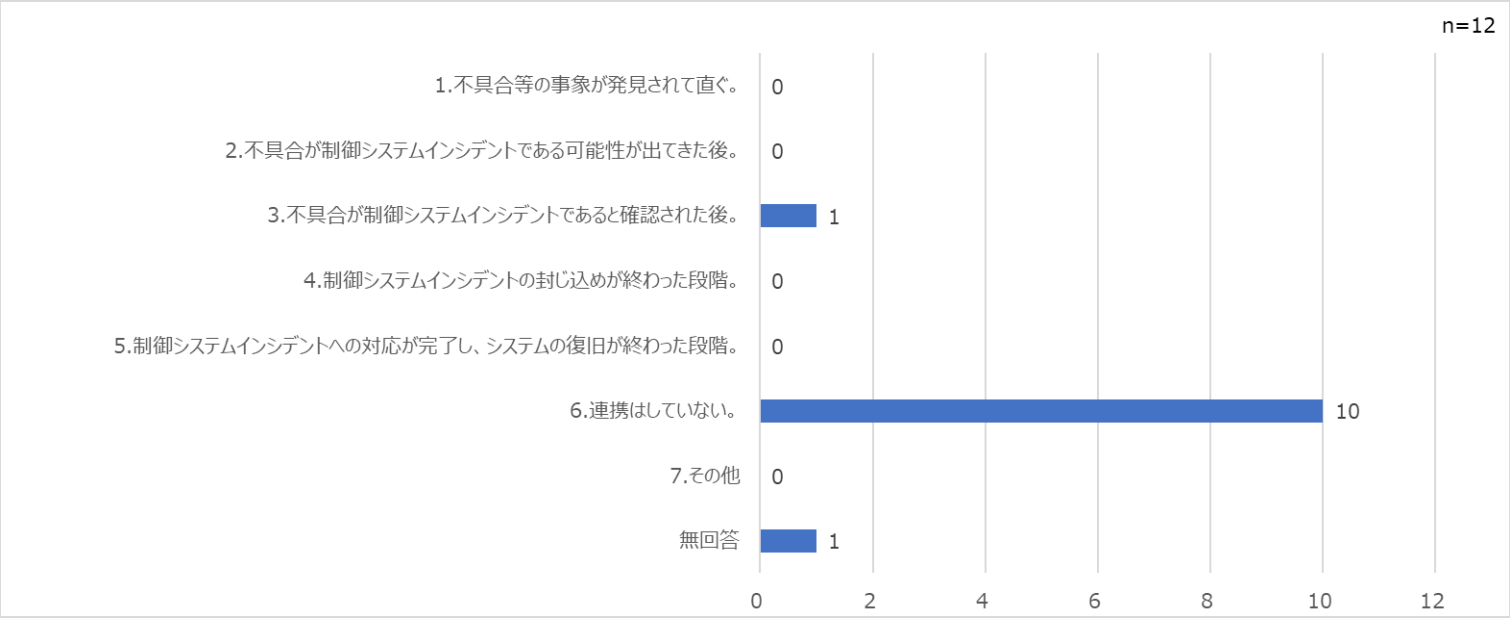
質問	その制御システムインシデントの発生に伴う、公的な窓口（所属するサイバーセキュリティ情報の共有団体（ISAC、セプター、業界団体等））への報告・連携（対応相談）の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-40

所管省庁への報告・連携のタイミング

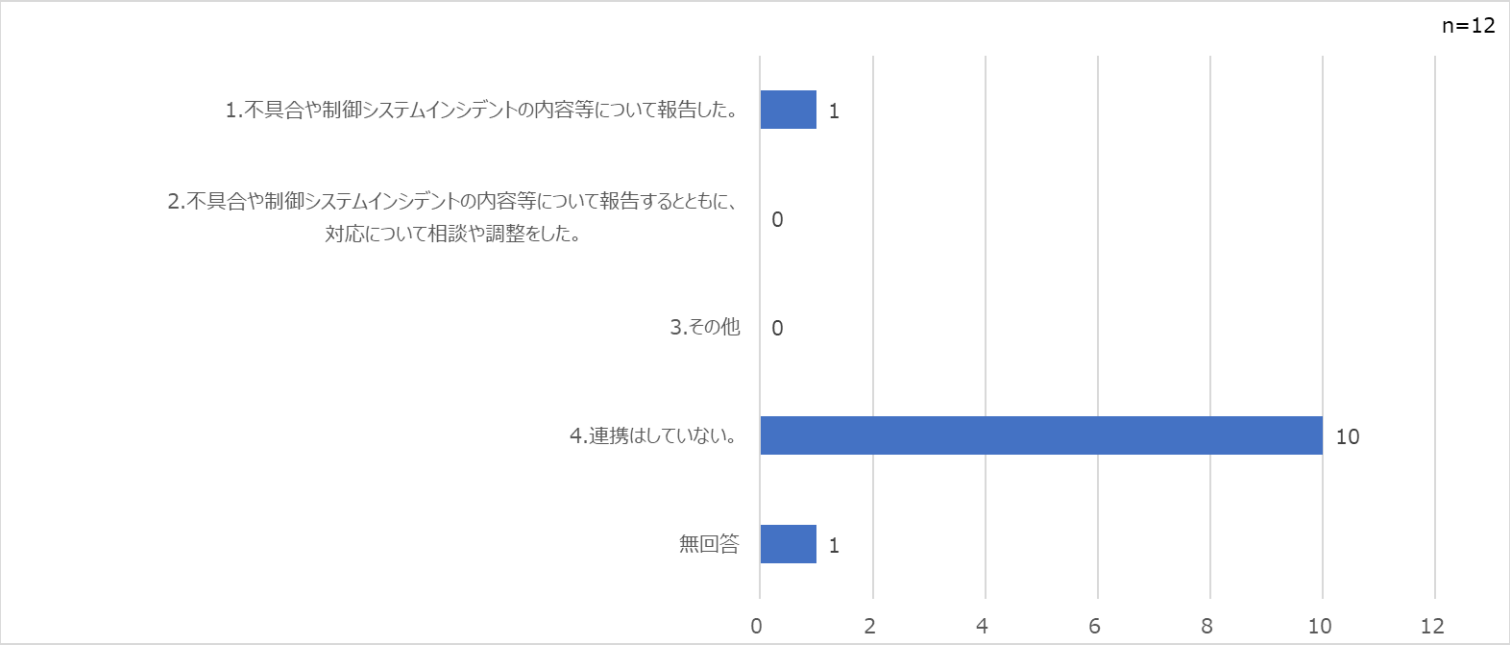
質問	その制御システムインシデントの発生に伴う、公的な窓口（所管省庁）への報告・連携（対応相談）のタイミングについてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-41

所管省庁への報告・連携の内容

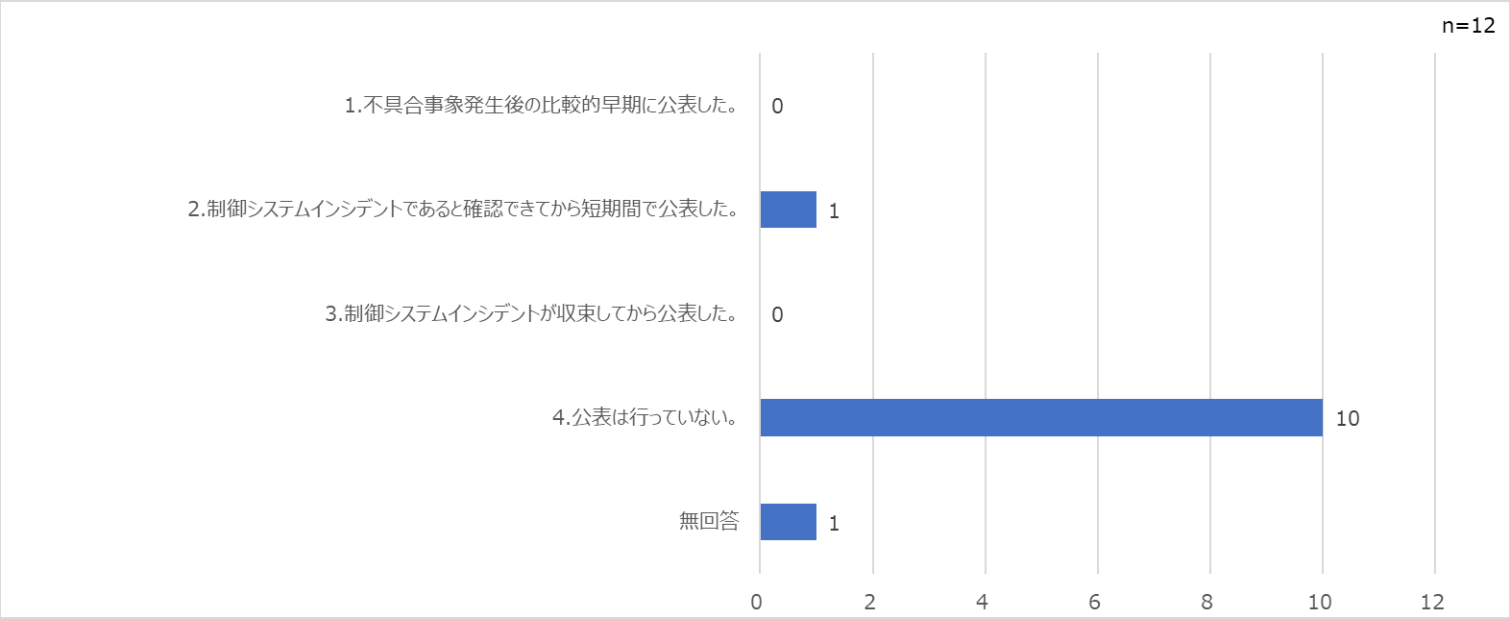
質問	その制御システムインシデントの発生に伴う、公的な窓口（所管省庁）への報告・連携（対応相談）の内容についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-3-42

インシデントの対外公表

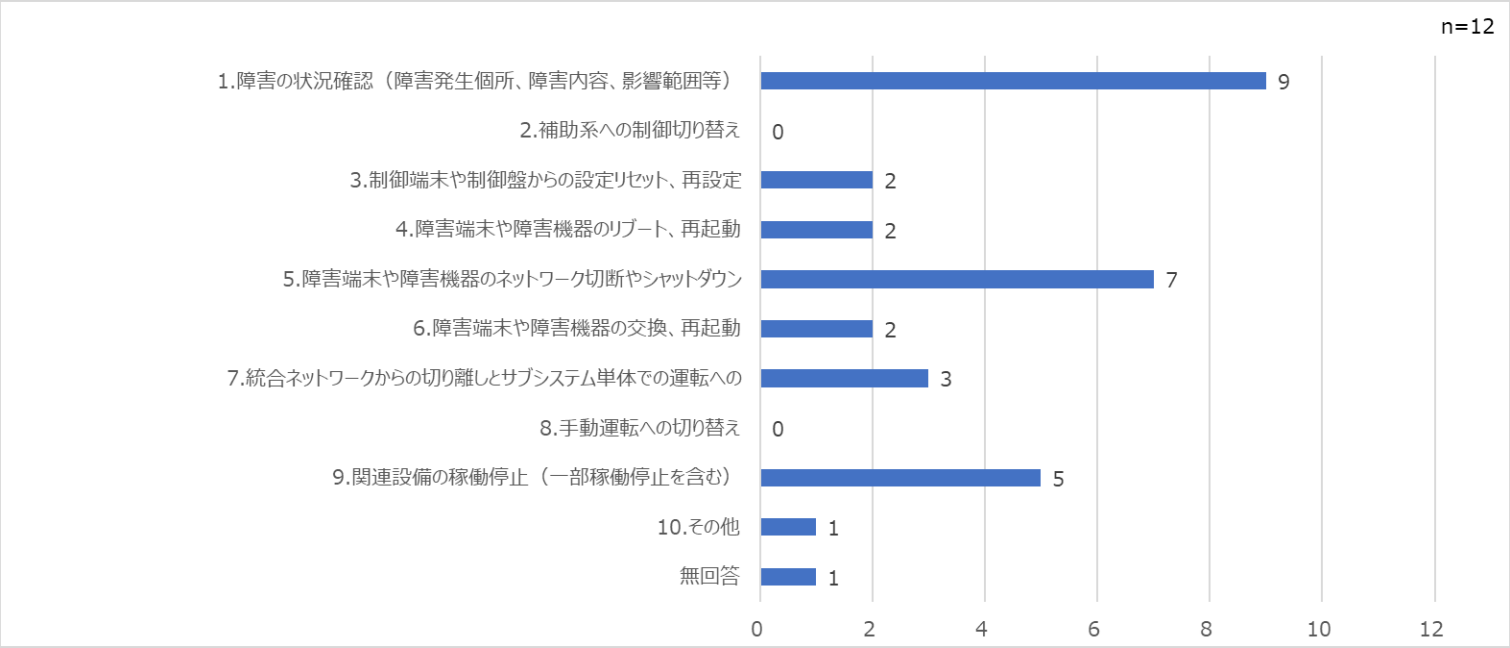
質問	その制御システムインシデントの発生に関して、対外公表（自社サイトでの公表やプレスリリース等）しましたか。
回答形態	単一回答
自由記述欄	なし



設問番号：5-4-1

事態収束のために実施した対処内容（1/2）

質問	その制御システムインシデントに関して、事態収束（初動対処に加え、事態の封じ込めまで）のために実施した対処内容についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-4-1

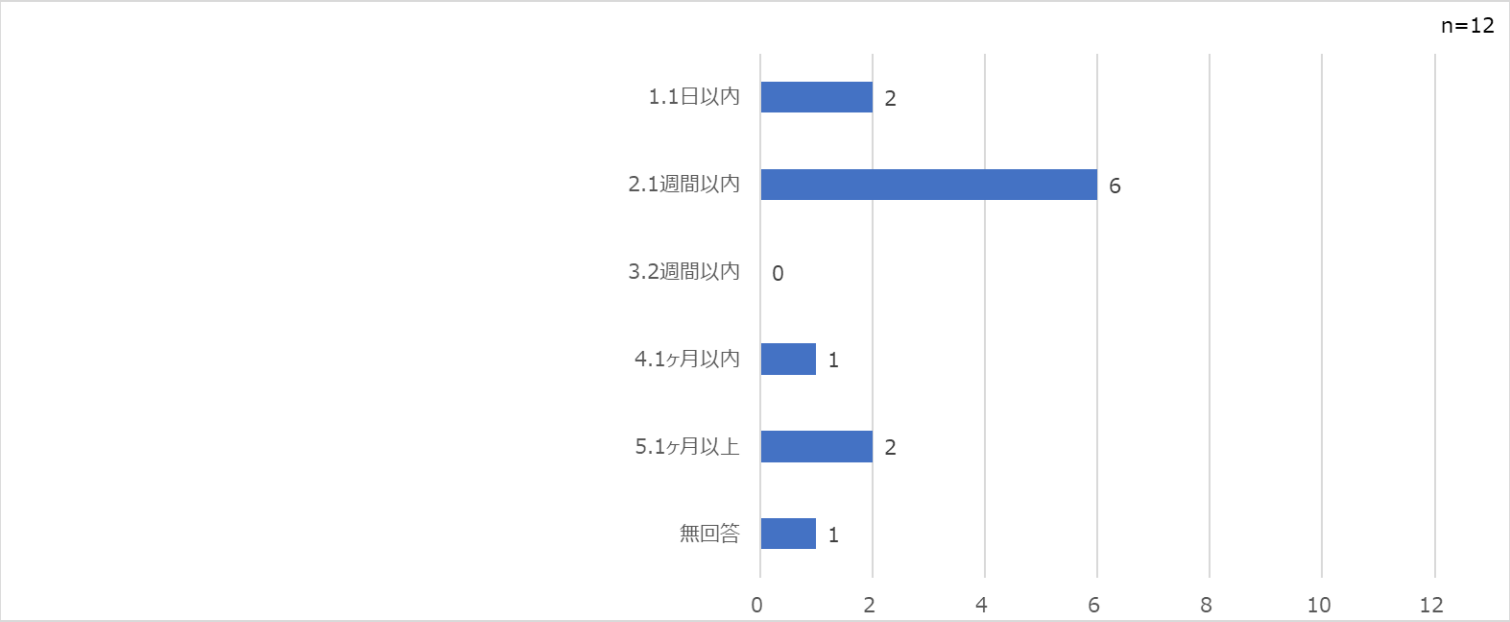
事態収束のために実施した対処内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 対象機器の初期化。

設問番号：5-4-2

事態収束のために要した期間

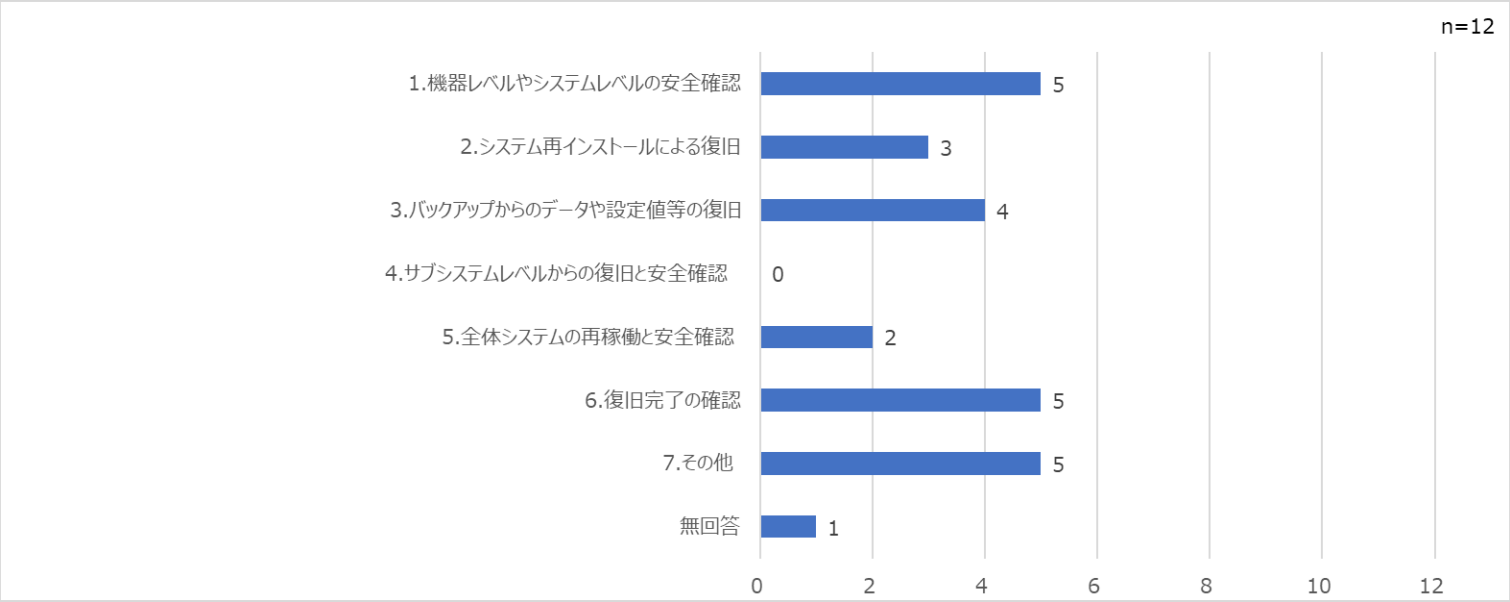
質問	その制御システムインシデントに関して、事態収束のために要した期間（事態の発生・発見からの期間）についてお答えください。
回答形態	単一回答
自由記述欄	なし



設問番号：5-4-3

システム復旧のために実施した対処内容（1/2）

質問	その制御システムインシデントに関して、システム復旧のために実施した対処内容についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-4-3

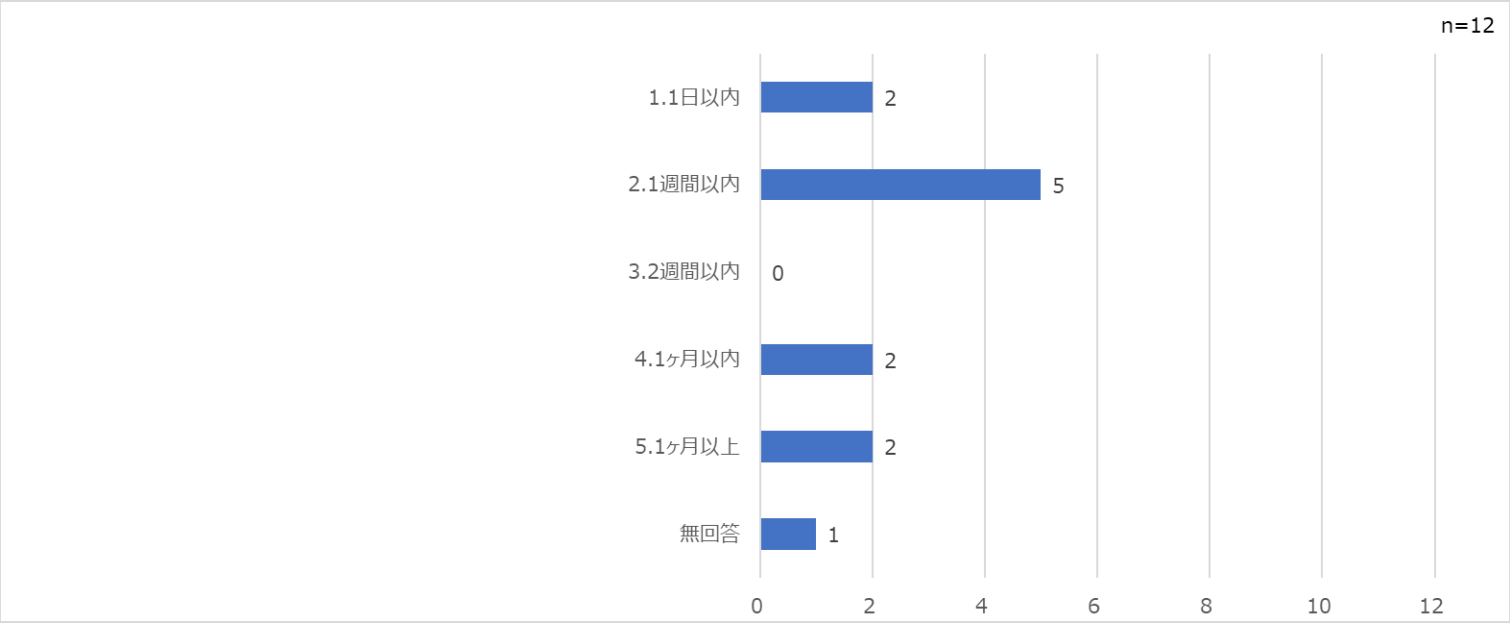
システム復旧のために実施した対処内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 感染した設備PCのウィルススキャンと駆除。 • 生産製品の改修。 • 当該システムの構成を変更し、インターネットとの接続を無くした。 • マルウェアの駆除のみ。OS再インストールはBCPの観点で行えていない。

設問番号：5-4-4

システム復旧のために要した期間

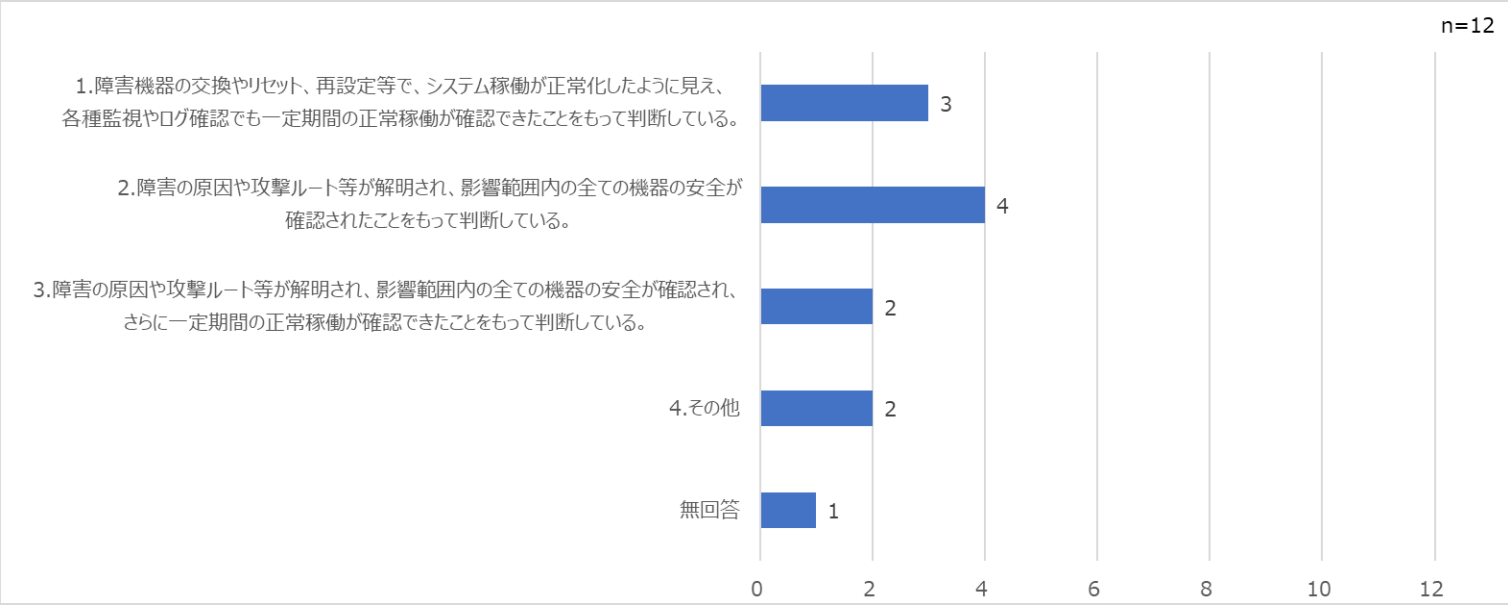
質問	その制御システムインシデントに関して、システム復旧のために要した期間（事態の発生・発見からの期間）についてお答えください。
回答形態	単一回答
自由記述欄	なし



設問番号：5-4-5

インシデントの収束判断（1/2）

質問	その制御システムインシデントが収束したとの判断はどのような基準で実施しましたか。
回答形態	複数回答
自由記述欄	あり



設問番号：5-4-5

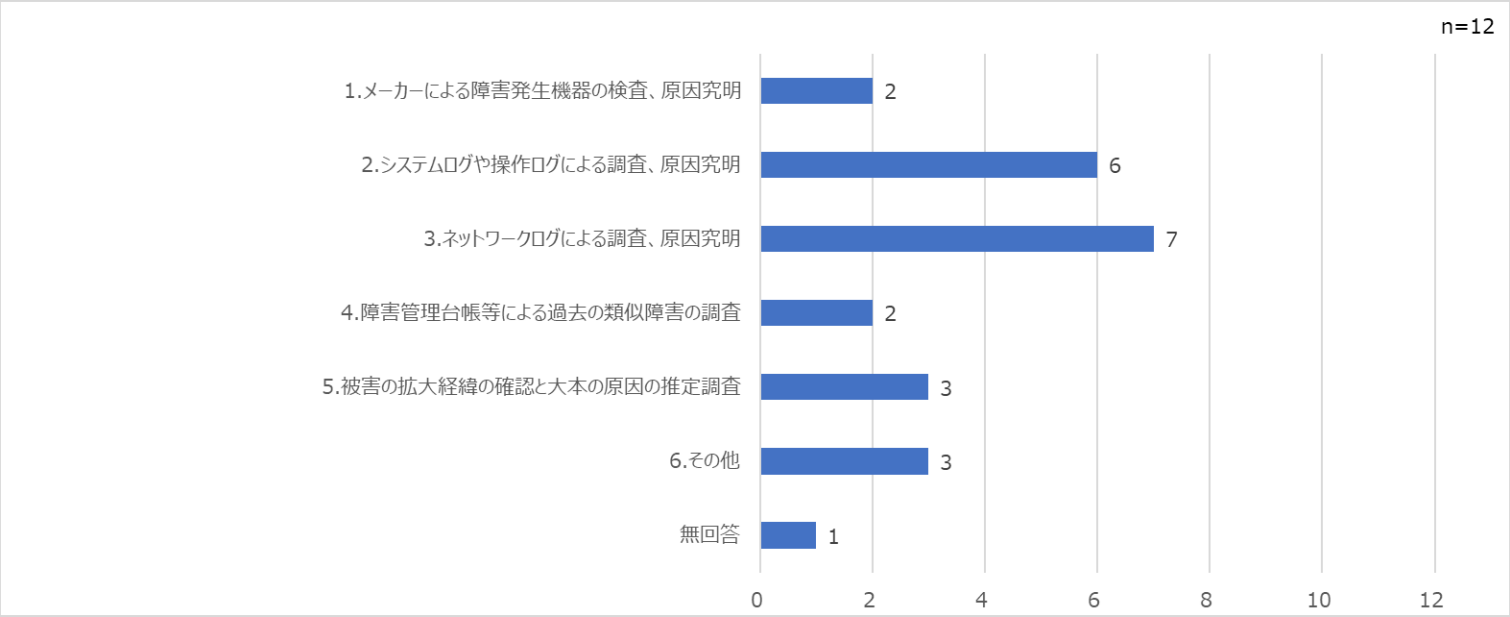
インシデントの収束判断（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• 機器の正常稼働。 • マルウェア駆除とネットワーク隔離。

設問番号：5-4-6

インシデント調査として実施した対処内容（1/2）

質問	その制御システムインシデントに対する事態解明調査として実施した対処内容についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-4-6

インシデント調査として実施した対処内容（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• EDRのログ調査のみ。 • USBチェック。 • 機器管理台帳の調査。

設問番号：5-4-7

インシデント対応について評価できる点

質問	その制御システムインシデントに関して、その対応を振り返って評価できると思った点についてお答えください。
回答形態	自由記述
回答数	9
個社回答	• chatで即時対応。 • 遠隔地の工場での障害発生現場と、本社のCSIRTメンバがコミュニケーション良く、比較的スムーズに対応にあたることができた。 • 各部門が連携しあい、迅速に対処が行えた。 • 気付いてからネットワーク遮断の判断は早かった。 • セキュリティに関する社内協議会での事例共有を実施した。 • セキュリティ部門に連絡があった段階で速やかに関係するネットワークを切断したこと。 • 調査段取り。 • 特に評価できる点はない。願わくばOS再インストールをしたいが、現場操業の関係で出来ていない点は改善点であると考える。 • 評価できる点はなし 海外工場での設備で使用するUSBメモリの管理状態が悪かった。

設問番号：5-4-8

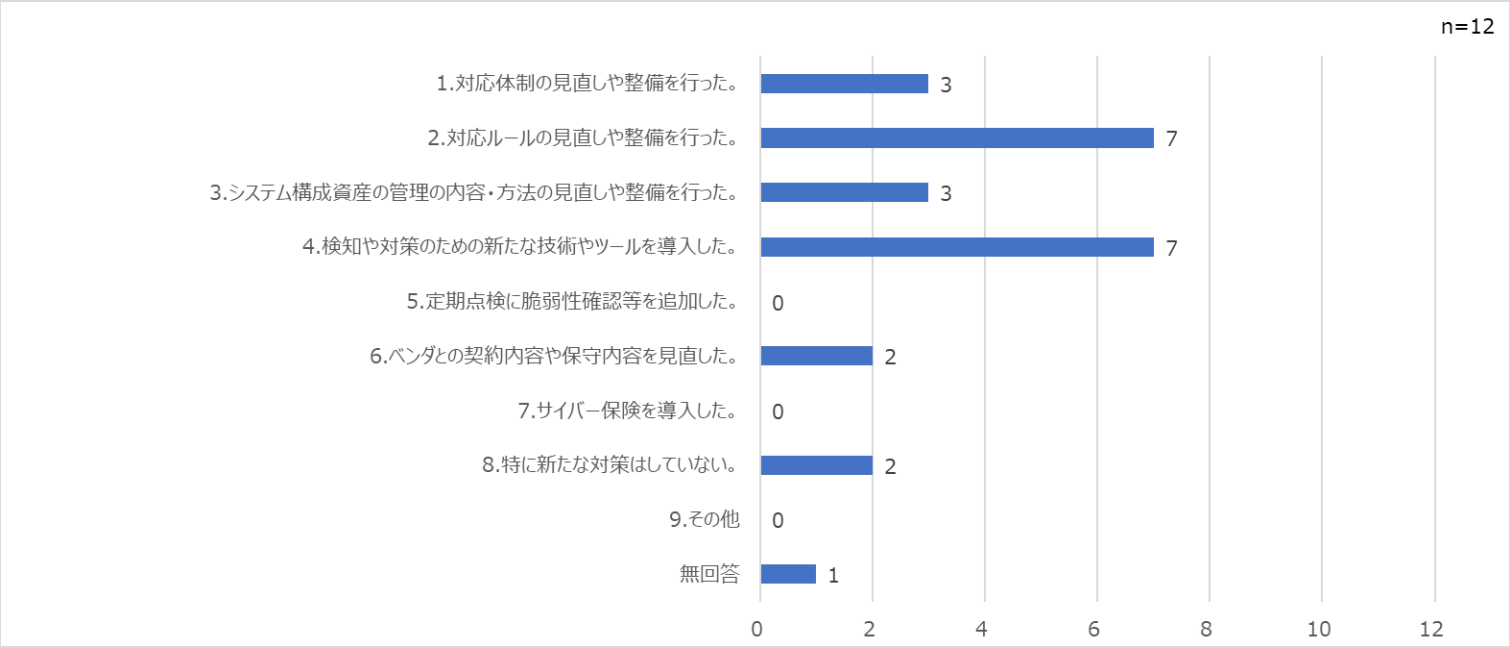
インシデント対応について課題と考える点

質問	その制御システムインシデントに関して、その対応を振り返って課題と思った点についてお答えください。
回答形態	自由記述
回答数	11
個社回答	• USBの事前ウィルスチェック。 • USBメモリ、および設備の管理、マルウェア対策が不十分だった。 • インシデント対応の体制や、対応フロー等が定まっていなかった。 • 各部門が連携しあい、迅速に対処が行えた。 • 現地対応支援メンバの工場への臨時入館がスムーズにできなかった。 • 情報システム部との情報共有が薄い。 • 制御系システムにおいても、ITと同様の障害が発生するため、セキュリティ対策が必要である点。 • セキュリティの専門知識を持っている人が少ない。インシデント対応を実施した実績のある人が少ない。 • セキュリティを全く考慮しない（する必要がなかった時代に建設）設備の存在。 • 対応人員に限りがあり、スピード復旧とはいかなかった。 • マルウェア感染端末のOS再インストールを実施できないこと。

設問番号：5-5-1

インシデント発生を受けて実施したセキュリティ対策

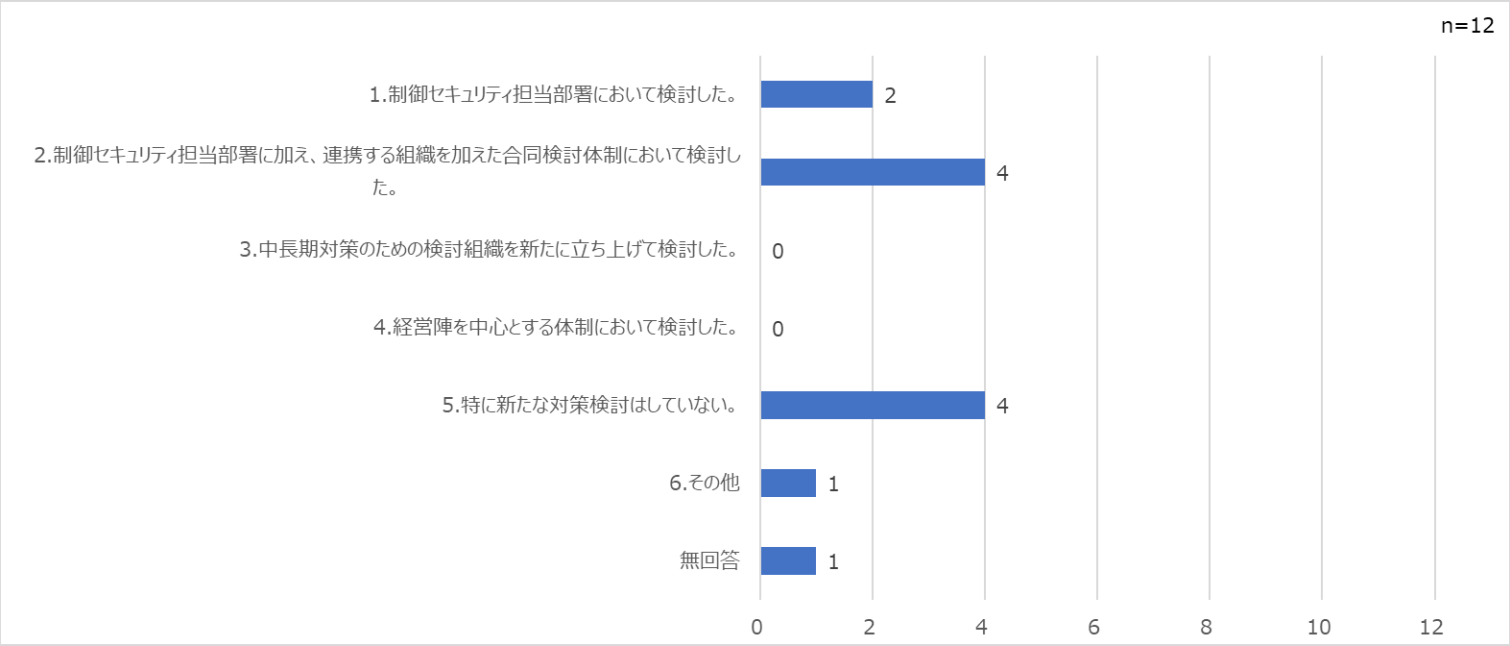
質問	その制御システムインシデントの発生を受けて実施した追加のセキュリティ対策があれば、その内容についてお答えください。
回答形態	複数回答
自由記述欄	あり



設問番号：5-5-2

インシデント発生の振り返りの検討体制（1/2）

質問	その制御システムインシデントの発生を受けて実施した追加のセキュリティ対策において、その検討体制についてお答えください。
回答形態	単一回答
自由記述欄	あり



設問番号：5-5-2

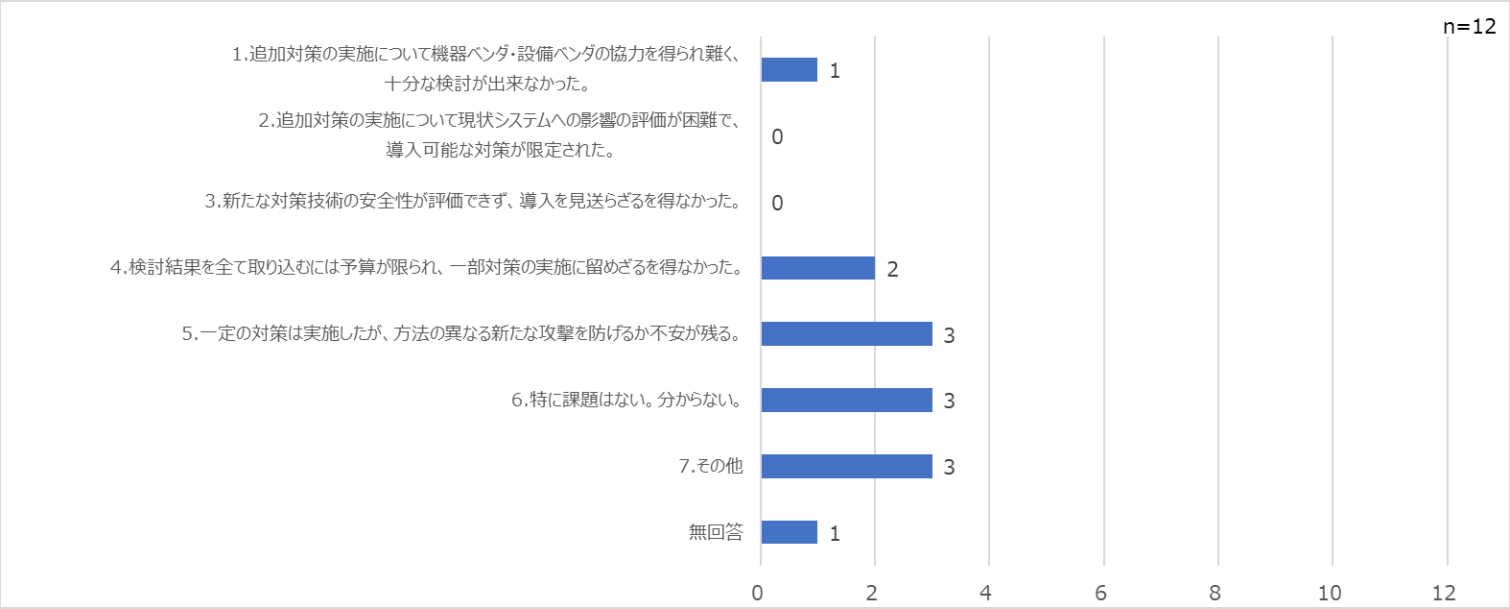
インシデント発生の振り返りの検討体制（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• EDR展開の促進。

設問番号：5-5-3

インシデント発生を受けて実施したセキュリティ対策における課題（1/2）

質問	その制御システムインシデントの発生を受けて実施した追加のセキュリティ対策の実施から見えた課題は何ですか？
回答形態	複数回答
自由記述欄	あり



設問番号：5-5-3

インシデント発生を受けて実施したセキュリティ対策における課題（2/2）

選択肢の内容	個社の回答（自由記述）
その他（具体的に）	• インターネットとの接続点については限られているので調査し、応急対策は実施し、新たな設置については対策なしにインターネット接続できなくしたが、今後増えるであろう外部接続に対し対応するマンパワーと費用の増大が懸念される。また、制御システムベンダーのセキュリティに対する姿勢のレベル差も懸念される。 • 海外拠点を含めたITガバナンスの難しさ。 • 制御系システムに関する対応体制、ルール等の必要性。